

FastIron Software Release 07.4.00p

Release Notes v1.0

April 12, 2016

Document History

Document Title	Summary of Changes	Publication Date
FastIron Software Release R07.4.00p Release Notes v1.0	Initial release	April 2016

Copyright © 2016 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, ClearLink, DCX, Fabric OS, HyperEdge, ICX, MLX, MyBrocade, OpenScript, VCS, VDX, Vplane, and Vyatta are registered trademarks, and Fabric Vision is a trademark of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of others.

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.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

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>.

Contents

Supported devices	7
Unsupported devices	7
Manageability	7
Summary of enhancements	8
Release 07.4.00p	8
Release 07.4.00n	8
Release 07.4.00m	8
Release 07.4.00k	8
Release 07.4.00j	8
Release 07.4.00h	8
Software enhancements	8
Release 07.4.00g	8
Release 07.4.00f	8
Release 07.4.00e	8
Release 07.4.00d1	8
Release 07.4.00d	8
Release 07.4.00c	9
Release 07.4.00b	9
Release 07.4.00a	9
Hardware enhancements	9
Software enhancements	9
Release 07.4.00	10
Hardware enhancements	10
Software enhancements	10
Summary of enhancements in TurboIron 24X 07.4.00	13

Configuration Notes and feature limitations.....	13
Note regarding Telnet and Internet Explorer 7	14
Note regarding US-Cert advisory 120541.....	14
Feature support for FCX, FESX6, ICX, SX, and FWS.....	15
Supported FSX modules	15
Supported management features	15
Supported security features.....	18
Supported system-level features	20
Supported Layer 2 features	23
Supported base Layer 3 features	26
Supported edge Layer 3 features	27
Supported full Layer 3 features	28
Supported IPv6 management features	30
Unsupported features	31
TurboIron 24X Feature Support.....	32
Supported Management Features	32
Supported IPv6 Management Features	33
Supported Security Features	34
Supported System-Level Features.....	35
Supported Layer 2 Features	38
Supported Layer 3 Features	40
Upgrading software for FSX, FESX6, FWS, FCX, and ICX	42
Important notes about upgrading the software.....	42
Important notes about downgrading the software.....	42
Standard upgrade procedure	42
Software image file for Release 07.4.00p	42
PoE Firmware files	43

Upgrading the boot code.....	44
Upgrading the flash code.....	44
Confirming software versions (IronStack devices).....	46
Troubleshooting a failed software image installation.....	47
Upgrading software for Turbolron 24X.....	47
Factory Pre-loaded Software.....	47
Upgrading software images	48
Upgrading the Boot Code	48
Upgrading the Flash Code	48
Technical support.....	48
Getting Help or reporting errors.....	49
E-mail and telephone access.....	49
Additional resources	49
Closed Defects.....	50
Customer reported defects closed with code in Release 07.4.00p.....	50
Customer reported defects closed with code in Release 07.4.00n.....	50
Customer reported defects closed with code in Release 07.4.00m.....	51
Customer reported defects closed with code in Release 07.4.00k.....	51
Customer reported defects closed with code in Release 07.4.00j	53
Customer reported defects closed with code in Release 07.4.00h.....	56
Customer reported defects closed with code in Release 07.4.00g	58
Customer reported defects closed with code in Release 07.4.00f.....	60
Customer reported defects closed with code in Release 07.4.00e	68
Customer reported defects closed with code in Release 07.4.00d1	74
Customer reported defects closed with code in Release 07.4.00d.....	74
Customer reported defects closed with code in Release 07.4.00c	83

Customer reported defects closed with code in Release 07.4.00b.....	89
Customer reported defects closed with code in Release 07.4.00a	90
Customer reported defects closed with code in Release 07.4.00	95
Customer reported defects closed without code in Release 07.4.00.....	104
Open defects.....	105
Open defects in Release 07.4.00a	105
Open defects in Release 07.4.00	107

Supported devices

This 07.4.00p software release applies to the following Brocade products:

- FCX Series (FCX)
- FastIron X Series:
 - o FastIron Edge Switch X Series, (IPv6 models) (FESX6)
 - o FastIron SX 800 and 1600 (FSX 800 and FSX 1600)
- FastIron WS Series (FWS)
- ICX 6610 Series (ICX 6610)
- ICX 6430 Series (ICX 6430)
- ICX 6450 Series (ICX 6450)
- Turbolron 24X (TI 24X)

Unsupported devices

This 07.4.00p software release does **not** support the following Brocade products:

- FastIron GS Series (FGS)
- FastIron LS Series (FLS)
- FastIron Edge (FES)
- FastIron Edge Switch X Series IPv4 models (FESX v4)
- FastIron SuperX

Manageability

This 07.4.00p software release is supported by Brocade Network Advisor 11.2.1. Any earlier versions of Network Advisor, as well as any version of IronView Network Manager are not compatible with this release or its supported hardware platforms (see Supported Devices). Network Advisor is generally available for download on my.brocade.com. It is strongly recommended that customers upgrade to Network Advisor 11.2.1, as part of their upgrade to this 07.4.00p software release.

Summary of enhancements

Release 07.4.00p

Release 07.4.00p contains defect fixes. There are no enhancements in this release.

Release 07.4.00n

Release 07.4.00n contains defect fixes. There are no enhancements in this release.

Release 07.4.00m

Release 07.4.00m contains defect fixes. There are no enhancements in this release.

Release 07.4.00k

Release 07.4.00k contains defect fixes. There are no enhancements in this release.

Release 07.4.00j

Release 07.4.00j contains defect fixes. There are no enhancements in this release.

Release 07.4.00h

Release 07.4.00h contains the following software enhancement and defect fixes.

Software enhancements

Feature	Description	Applicable devices	See <i>FastIron Document Update Guide</i> , section entitled...
Stack guard	Disables stacking control traffic on non-stacking ports.	FCX ICX 6430 ICX 6450	Configuring stack guard.

Release 07.4.00g

Release 07.4.00g contains defect fixes for ICX 6610 devices. There are no enhancements in this release.

Release 07.4.00f

Release 07.4.00f contains defect fixes. There are no enhancements in this release.

Release 07.4.00e

Release 07.4.00e contains defect fixes. There are no enhancements in this release.

Release 07.4.00d1

Release 07.4.00d1 contains Turbolron 24X defect fixes. There are no enhancements in this release.

Release 07.4.00d

Release 07.4.00d contains defect fixes. There are no enhancements in this release.

Release 07.4.00c

Release 07.4.00c contains defect fixes. Also, the “show link-aggregate partner” has been added to this release to provide information about LAG partners. Refer to the February 22, 2013 issue of the *FastIron Family Documentation Updates* for details.

Release 07.4.00b

Releases 07.4.00b contains defect fixes. There are no enhancements in these releases.

Release 07.4.00a

Hardware enhancements

There are no hardware enhancements in Release 07.4.00a.

Software enhancements

Feature	Description	Applicable devices	See <i>FastIron Configuration Guide</i> , section entitled...
Stacking configuration for ICX 6430	This release supports including ICX 6430 48-port units and ICX 6430 24-port stacking units in an IronStack.	ICX 6430	Connecting ICX 6450 and ICX 6430 devices in a stack Configuring an ICX 6450 and ICX 6430 IronStack
IPv6 routing features	This release adds the following IPv6 routing features: <ul style="list-style-type: none">• IPv6 static routes• ECMP load sharing	ICX 6450	Static IPv6 route configuration ECMP load sharing for IPv6

Release 07.4.00

Hardware enhancements

Feature	Description	Applicable devices	See <i>FastIron Configuration Guide</i> , section entitled...
New hardware	<p>This release introduces the new Brocade ICX 6430 and ICX 6450 Series stackable switches. The following optics are supported on these devices:</p> <ul style="list-style-type: none">• E1MG-TX• E1MG-SX-OM 1000Base-SX SFP optic• E1MG-LX-OM 1000Base-LX SFP optic• E1MG-LHA-OM 1000Base-LHA SFP optic• E1MG-LHB 1000Base-LHB SFP optic• 10G-SFPP-SR 10GBASE-SR, SFP+ optic (LC)• 10G-SFPP-LR 10GBASE-LR, SFP+ optic (LC)• 10G-SFPP-LRM 10GBASE-LRM, 1310NM SFP+ OPTIC (LC),• 10G-SFPP-ER 10GBASE-ER SFP+ optic (LC)• 10G-SFPP-USR (ICX 6450 only)• 1G-SFP-TWX-0101, 1G-SFP-TWX-0501• 10G-SFPP-TWX-0101, 10G-SFPP-TWX-0301, 10G-SFPP-TWX-0501	<ul style="list-style-type: none">• ICX 6430• ICX 6450	<p>Brocade ICX 6430 and ICX 6450 Series Hardware Installation Guide</p> <p>and</p> <p>http://www.brocade.com/downloads/documents/data_sheets/product_data_sheets/Optics_DS.pdf</p>
New Optic	<p>The new 10Gbps USR (Ultra Short Reach) SFP+(10G-SFPP-USR) is now available for platforms that have 10Gbps SFP+ ports.</p>	<ul style="list-style-type: none">• FCX• FSX devices that have SX-FI-8XG or SX-FI-2XG modules installed• ICX 6610• ICX 6450• Turbolron 24X	<p>http://www.brocade.com/downloads/documents/data_sheets/product_data_sheets/Optics_DS.pdf</p>

Software enhancements

Feature	Description	Applicable devices	See <i>FastIron Configuration Guide</i> , section entitled...
Multi-Chassis Trunking	<p>Multi-Chassis Trunking (MCT) is technology that allows multiple switches to appear as single logical switch connecting to another switch using a standard trunk group. MCT is supported on FSX devices that have any of the following modules installed.</p> <ul style="list-style-type: none">• SX-FI-24GPP• SX-FI-24HF• SX-FI-2XG• SX-FI-8XG• SX-FI48GPP <p>These modules must be used for Inter-Chassis Links and Cluster Customer Edge Ports.</p>	<ul style="list-style-type: none">• FSX 800• FSX 1600	<p>Multi-Chassis Trunking (MCT)</p>

Feature	Description	Applicable devices	See <i>FastIron Configuration Guide</i> , section entitled...
MAC address move notification	MAC address movement notification allows you to monitor the movement of MAC addresses that migrate from port to port. It enables you to distinguish between legitimate movement and malicious movement by allowing you to define malicious use as a threshold number of times a MAC address moves within a specific interval.	<ul style="list-style-type: none"> • FCX • FESX6 (IPv6 models) • FSX 800 • FSX 1600 • ICX 6610 • ICX 6430 • ICX 6450 	Monitoring MAC address movement
Maximum Trunk support and Maximum trunk port member support on FastIron SX interface modules	<p>The following Interface modules support up to 12 ports per trunk group on the FastIron SX chassis for both static and LACP trunks. A maximum of 256 trunks are supported only when the following modules and zero-port management modules are installed on the chassis:</p> <ul style="list-style-type: none"> • SX-FI48GPP—48-port 10/100/1000 Mbps Ethernet PoE/POE+ interface module • SX-FI-24GPP—24-port Gigabit Ethernet copper interface module • SX-FI-24HF—24-port Gigabit Ethernet fiber interface module • SX-FI-2XG—2-port 10 Gigabit Ethernet interface module • SX-FI-8XG—8-port 10 Gigabit Ethernet interface module 	<ul style="list-style-type: none"> • FSX 800 • FSX 1600 	Trunk Groups and Dynamic Link Aggregation
VRRP-E short-path forwarding and revertible option	Also known as 'VRRP-E Extension for Server Virtualization,' enables the Brocade device to bypass the master router and directly forward packets to their destination through interfaces on the backup router. If enabled, the traffic travels through the short-path forwarding (SPF) path to reach the client.	<ul style="list-style-type: none"> • FSX 800 • FSX 1600 	VRRP and VRRP-E
CPU rate-limiting	Increases CPU efficiency by preventing unnecessary traffic from being sent to the CPU and by limiting the rate at which some packet types are delivered to the CPU.	<ul style="list-style-type: none"> • FCX • FESX6 (IPv6 models) • FSX 800 • FSX 1600 • ICX 6610 • ICX 6430 • ICX 6450 	CPU rate-limiting
Support for 16K Nexthops	<p>16,000 nexthops are supported on the following modules:</p> <ul style="list-style-type: none"> • SX-FI-24GPP • SX-FI-24HF • SX-FI-2XG • SX-FI-8XG • SX-FI48GPP 	<ul style="list-style-type: none"> • FSX 800 • FSX 1600 	Chapter 28, Base Layer 3 and Routing Protocols

Feature	Description	Applicable devices	See <i>FastIron Configuration Guide</i> , section entitled...
Quality of Service (QoS) support for ICX 6430 and 6450 switches	Differences are detailed for the ICX 6430 switch in the following areas: <ul style="list-style-type: none"> • Priority to hardware forwarding queue mapping • Default QoS mappings • Default values for scheduling type • Default scheduling configuration 	<ul style="list-style-type: none"> • ICX 6430 • ICX 6450 	Quality of Service
Dynamic buffer support for 6430 and 6450 switches	Specific information is provided for the 6430 and 6450 switches in the following areas: <ul style="list-style-type: none"> • Port and buffer descriptor values • Buffer sharing levels • Configuring values for the ICX 6430 	<ul style="list-style-type: none"> • ICX 6430 • ICX 6450 	Basic Layer 2 Features
Stacking configuration for ICX 6430 and ICX 6450 devices	ICX 6430 and ICX 6450 devices have four ports on the front panel for stacking configuration. NOTE: ICX 6430 and ICX 6450 units cannot co-exist in the stack. ICX 6430 and ICX 6450 devices support linear and ring stack topologies, and can also operate as standalone devices. When stacking is enabled, ports 1 and 3 are dedicated to stacking and cannot be used for data ports. If stacking is not enabled on the ports, then all four stacking ports can be used for data or uplink ports.	<ul style="list-style-type: none"> • ICX 6430 • ICX 6450 	Connecting ICX 6450 and ICX 6430 devices in a stack Configuring an ICX 6450 and ICX 6430 IronStack
Auto Image Copy for stack units	The Auto Image Copy feature ensures that all units in a stack are running the same flash image after a stack merge. This feature is introduced on the ICX and FCX devices.	<ul style="list-style-type: none"> • FCX • ICX 6610 • ICX 6430 • ICX 6450 	Auto Image Copy for stack units
Software licensing enhancements	Software-based licensing is introduced on the ICX 6450 devices. The premium license is available on the ICX 6450 devices.	ICX 6450	Software-based Licensing
Licensing for Ports on Demand	Licensing for Ports on Demand (POD) is introduced on the ICX 6450 devices. The ICX 6450 device has four active uplink ports on slot 2. By default, ports 1 and 3 are 10 Gbps ports and ports 2 and 4 are 1 Gbps ports. To increase the uplink capacity for two ports (ports two and four) from 1 Gbps to 10 Gbps port speed, purchase the ICX6450-2X10G-LIC-POD license. The PoD feature is not applicable to ICX 6430 devices because there are no 10 Gbps ports on the device.	ICX 6450	Licensed features and part numbers Licensing for Ports on Demand
31-bit subnet mask	31-bit subnet masks can be configured on point-to-point interfaces.	FSX, FCX, and ICX 6610 devices running full Layer 3 image	Configuring 31-bit subnet masks on point-to-point networks

Feature	Description	Applicable devices	See <i>FastIron Configuration Guide</i> , section entitled...
Web Management Interface	Support for the Web Management Interface on the ICX 6430 and ICX 6450 devices.	<ul style="list-style-type: none"> ICX 6430 ICX 6450 	See the document: <i>Brocade FCX, Brocade FastIron SX, Brocade ICX Web Management Interface User Guide</i>
MIB enhancement	Support for the registration MIBs on the ICX 6430 and ICX 6450 devices.	<ul style="list-style-type: none"> ICX 6430 ICX 6450 	Unified IP MIB Reference
Diagnostic information	New CLI command: supportsave	<ul style="list-style-type: none"> ICX 6430 ICX 6450 	Brocade FastIron, FCX, ICX, Turbolron Diagnostic and Troubleshooting Reference
Diagnostic information	New Reliability, Availability and Serviceability debug commands	<ul style="list-style-type: none"> FCX FSX 800 FSX 1600 ICX 6610 	Brocade FastIron, FCX, ICX, Turbolron Diagnostic and Troubleshooting Reference
VLAN-based mirroring and sFlow with mirroring on the same port	Support for VLAN-based mirroring for FastIron X Series modules: <ul style="list-style-type: none"> SX-FI-24GPP SX-FI-24HF SX-FI-2XG SX-FI-8XG SX-FI48GPP 	<ul style="list-style-type: none"> FSX 800 FSX 1600 	VLAN-based mirroring on FastIron X Series devices
802.1x user name support	802.1x user name support for RADIUS accounting messages.	<ul style="list-style-type: none"> FCX FESX6 (IPv6 models) FSX 800 FSX 1600 ICX 6610 ICX 6430 ICX 6450 	Support for RADIUS user-name attribute in access-accept messages

Summary of enhancements in Turbolron 24X 07.4.00

Feature	Description	See the <i>Turbolron 24X Configuration Guide</i> , section entitled...
31-bit subnet mask	31-bit subnet masks can be configured on point-to-point interfaces.	Configuring 31-bit subnet masks on point-to-point networks

Configuration Notes and feature limitations

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

- FastIron 07.4.00 and later softwares are supported on FWS switches, but none of the feature enhancements listed earlier in the document are available in these devices.

- FastIron 07.4.00 and later softwares are supported on Turbolron switches, but only the 31-bit subnet mask feature among the list of enhancements is available on these devices.
- ICX 6430 devices support only up to 4 devices in an IronStack, while up to eight ICX 6450 devices can be included in a stacking configuraton.

NOTE: ICX 6430 and ICX 6450 can not co-exist in a stack.

- ICX 6430 and ICX 6450 devices support only one boot sequence from config terminal.
- On ICX 6430 and ICX 6450 devices, the **crypto key generate** command can take up to 30 minutes to complete.
- Brocade FastIron devices support RFC 2526, which requires that within each subnet, the highest 128 interface identifier values reserved for assignment as subnet anycast addresses. Thus, if you assign individual IPv6 addresses within a subnet, the second highest IPv6 address in the subnet does not work.

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-ssl3-tls-vulnerability-mitm.html>

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

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

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

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

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.

Supported management features

Table 1 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 1 Supported management features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
802.1X accounting	Yes	Yes	Yes	Yes	Yes
AAA support for console commands	Yes	No	Yes	Yes	Yes
Access Control Lists (ACLs) for controlling management access	Yes	Yes	Yes	Yes	Yes
Alias command	Yes	Yes	Yes	Yes	Yes
Combined DSCP and internal marking in one ACL rule	Yes	No	No	No	No

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
Single source address for the following packet types: <ul style="list-style-type: none"> • Telnet • TFTP • Syslog • SNMP • TACACS/TACACS+ • RADIUS • SSH • SNMP 	Yes	No	No	No	No
DHCP client-based auto-configuration	Yes	Yes	Yes	Yes	Yes
DHCP server	Yes	Yes	Yes	Yes	Yes
Disabling TFTP access	Yes	No	Yes	Yes	Yes
Brocade Network Advisor 11.2	Yes	Yes	Yes	Yes	Yes
Hitless management: <ul style="list-style-type: none"> • Hitless switchover • Hitless failover • Hitless OS upgrade 	Yes (FSX 800 and FSX 1600 only)	No	See next line item	See next line item	See next line item
Hitless stacking management: <ul style="list-style-type: none"> • Hitless stacking switchover • Hitless stacking failover 	NA	No	Yes	Yes	Yes
Hitless support for: <ul style="list-style-type: none"> • PBR • GRE Tunnels 	Yes (FSX 800 and FSX 1600 only)	No	Yes (PBR and GRE only)	Yes (PBR only)	No
Multi-chassis Trunking Supported on FSX devices that have the following modules: <ul style="list-style-type: none"> • SX-FI-24GPP • SX-FI-24HF • SX-FI-2XG • SX-FI-8XG • SX-FI48GPP 	Yes (FSX 800 and FSX 1600 only)	No	No	No	No
Remote monitoring (RMON)	Yes	Yes	Yes	Yes	Yes
Retaining Syslog messages after a soft reboot	Yes	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
sFlow support for IPv6 packets	Yes	Yes	Yes	Yes	ICX 6450 only
DHCP Client	Yes	Yes	Yes	Yes	Yes
SNTP Server	Yes	Yes	Yes	Yes	Yes
SNTP Client (Broadcast & Unicast)	Yes	No	Yes	Yes	Yes
Flexible Port On Demand Licensing	No	No	No	Yes	ICX 6450 only
sFlow version 2	Yes	Yes	Yes	Yes	ICX 6450 only
sFlow version 5 (default)	Yes	Yes	Yes	Yes	ICX 6450 only
Industry-standard Command Line Interface (CLI), including support for: <ul style="list-style-type: none"> Serial and Telnet access Alias command On-line help Command completion Scroll control Line editing Searching and filtering output Special characters 	Yes	Yes	Yes	Yes	Yes
Show log on all terminals	Yes	Yes	Yes	Yes	Yes
SNMP v1, v2, v3	Yes	Yes	Yes	Yes	Yes
SNMP V3 traps	Yes	Yes	Yes	Yes	Yes
Specifying the maximum number of entries allowed in the RMON Control Table	Yes	No	Yes	Yes	Yes
Specifying which IP address will be included in a DHCP/BOOTP reply packet	Yes	No	Yes	Yes	Yes
Traffic counters for outbound traffic	Yes	No	No	No	No
Web-based GUI	Yes	Yes	Yes	Yes	Yes
Web-based management HTTPS/SSL	Yes	Yes	Yes	Yes	Yes

Supported security features

Table 2 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 2 Supported security features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
802.1X port security	Yes	Yes	Yes	Yes	Yes
802.1X authentication RADIUS timeout action	Yes	Yes	Yes	Yes	Yes
802.1X dynamic assignment for ACL, MAC filter, and VLAN	Yes	Yes	Yes	Yes	Yes
Access Control Lists (ACLs) for filtering transit traffic					
• Support for inbound ACLs.	Yes	Yes	Yes	Yes	Yes
• Support Outbound ACLs	Yes *	No	Yes	Yes	Yes
(*FSX 800 and FSX 1600 on third-generation modules only)					
Address locking (for MAC addresses)	Yes	Yes	Yes	Yes	Yes
AES Encryption for SNMP v3	Yes	Yes	Yes	Yes	Yes
AES Encryption for SSH v2	Yes	Yes	Yes	Yes	Yes
Authentication, Authorization and Accounting (AAA):	Yes	Yes	Yes	Yes	Yes
• RADIUS					
• TACACS/TACACS+					
Denial of Service (DoS) attack protection:	Yes	Yes	Yes	Yes	Yes
• Smurf (ICMP) attacks					
• TCP SYN attacks					
DHCP Snooping	Yes	Yes	Yes	Yes	Yes
Dynamic ARP Inspection	Yes	Yes	Yes	Yes	Yes
EAP Pass-through Support	Yes	Yes	Yes	Yes	Yes
HTTPS	Yes	Yes	Yes	Yes	Yes
IP Source Guard	Yes	Yes	Yes	Yes	Yes
Local passwords	Yes	Yes	Yes	Yes	Yes
MAC address filter override of 802.1X	Yes	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
MAC address filtering (filtering on source and destination MAC addresses)	Yes	Yes	Yes	Yes	Yes
Ability to disable MAC learning	Yes	Yes	Yes	Yes	Yes
Flow-based MAC address learning	Yes	No	Yes	No	No
MAC port security	Yes	Yes	Yes	Yes	Yes
MAC address movement	Yes	No	Yes	Yes	Yes
Multi-device port authentication	Yes	Yes	Yes	Yes	Yes
Support for Multi-Device Port Authentication together with:					
• Dynamic VLAN assignment	Yes	Yes	Yes	Yes	Yes
• Dynamic ACLs	Yes	Yes	Yes	Yes	Yes
• 802.1X	Yes	Yes	Yes	Yes	Yes
• Dynamic ARP inspection with dynamic ACLs	Yes	No	No	No	No
• DHCP snooping with dynamic ACLs	Yes	No	No	No	No
• Denial of Service (DoS) attack protection	Yes	No	Yes	Yes	Yes
• Source guard protection	Yes	Yes	Yes	Yes	Yes
• ACL-per-port-per-VLAN	Yes	Yes	Yes	Yes	Yes
Multi-device port authentication password override	Yes	Yes	Yes	Yes	Yes
Multi-device port authentication RADIUS timeout action	Yes	Yes	Yes	Yes	Yes
Secure Copy (SCP)	Yes	Yes	Yes	Yes	Yes
Secure Shell (SSH) v2	Yes	Yes	Yes	Yes	Yes
Packet filtering on TCP Flags	No	Yes	Yes	Yes	Yes
DHCP Relay Agent information (DHCP Option 82)	Yes	Yes	Yes	Yes	ICX 6450 only
Web Authentication	Yes	Yes	Yes	Yes	Yes

Supported system-level features

Table 3 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 3 Supported system-level features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
10/100/1000 port speed	Yes	Yes	Yes	Yes	Yes
8,000 MAC addresses per switch	Yes	Yes	Yes	Yes	Yes
32,000 MAC addresses per switch	Yes	No	Yes	Yes	No
ACL-based mirroring	Yes	Yes	Yes	Yes	Yes
ACL-based fixed rate limiting	Yes	Yes	Yes	Yes	Yes
ACL-based adaptive rate limiting	Yes	No	Yes	Yes	Yes
ACL filtering based on VLAN membership or VE port membership	Yes	Yes	Yes	Yes	Yes
ACL logging of denied packets (IPv4)	Yes	Yes	Yes	Yes	Yes
ACL statistics	Yes	Yes	Yes	Yes	Yes
ACLs to filter ARP packets	Yes	Yes	Yes	Yes	No
Auto MDI/MDIX detection	Yes	Yes	Yes	Yes	Yes
Auto-negotiation	Yes	Yes	Yes	Yes	Yes
Automatic removal of Dynamic VLAN for 802.1X ports	Yes	Yes	Yes	Yes	Yes
Automatic removal of Dynamic VLAN for MAC authenticated ports	Yes	No	No	No	Yes
Byte-based broadcast, multicast, and unknown-unicast rate limits	Yes	No	No	No	No
Packet-based broadcast, multicast, and unknown-unicast rate limits	Yes	Yes	Yes	Yes	Yes
DiffServ support	Yes	Yes	Yes	Yes	Yes
Digital Optical Monitoring	Yes	Yes	Yes	Yes	Yes
Displaying interface names in Syslog messages	Yes	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
Displaying TCP and UDP port numbers in Syslog messages	Yes	Yes	Yes	Yes	Yes
Dynamic buffer allocation for QoS priorities	Yes	Yes	Yes	Yes	Yes
Flow control	Yes	Yes	Yes	Yes	Yes
Inbound rate limiting (port-based fixed rate limiting on inbound ports)	Yes	Yes	Yes	Yes	Yes
Foundry Discovery Protocol (FDP) / Cisco Discovery Protocol (CDP)	Yes	Yes	Yes	Yes	Yes
Generic buffer profile	No	Yes	Yes	Yes	Yes
Layer 2 hitless switchover and Layer 2 hitless failover NOTE: For details about this feature, refer to the <i>Brocade FastIron X Series Chassis Hardware Installation Guide</i>	Yes (FSX 800 and FSX 1600 only)	No	Yes	Yes	Yes
LLDP	Yes	Yes	Yes	Yes	Yes
LLDP-MED	Yes	Yes	Yes	Yes	Yes
MAC address filter-based mirroring	No	Yes	Yes	Yes	Yes
Multi-port static MAC address	Yes	Yes	Yes	Yes	Yes
Multiple Syslog server logging (up to six Syslog servers)	Yes	Yes	Yes	Yes	Yes
Outbound rate limiting (port-based and port- and priority-based rate limiting on outbound ports)	No	Yes	No	No	Yes
Outbound rate shaping	Yes	No	Yes	Yes	Yes
Path MTU Discovery	Yes	No	Yes	Yes	No
Port flap dampening	Yes	Yes	Yes	Yes	Yes
Port mirroring and monitoring (mirroring of both inbound and outbound traffic on individual ports)	Yes	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
Power over Ethernet (POE) IEEE 802.3af-2003 compliant	Yes (POE-enabled Interface modules with POE power supply)	Yes (FWS-POE and FWS- G-POE only)	Yes (FCX-S- HPOE only)	Yes ICX 6610- 24P and ICX 6610- 48P	Yes ICX 6450- 24P ICX 6450- 48P ICX 6430- 24P ICX 6430- 48P
High Power over Ethernet (POE)+ IEEE 802.3at-2009 compliant	Yes (SX- FI48GPP SX-FI- 24GPP module only)	No	Yes (FCX-S- HPOE only)	Yes ICX 6610- 24P and ICX 6610- 48P	Yes ICX 6450- 24P ICX 6450- 48P ICX 6430- 24P ICX 6430- 48P
PoE firmware upgrade via CLI	Yes	No	Yes	Yes	Yes
Priority mapping using ACLs	Yes	Yes	Yes	Yes	Yes
Protected link groups	Yes	Yes	Yes	Yes	Yes
Layer 2 stacking rapid failover and switchover	NA	No	Yes	Yes	Yes
Static MAC entries with option to set traffic priority	Yes	Yes	Yes	Yes	Yes
Symmetric flow control <ul style="list-style-type: none"> Can transmit and receive 802.3x PAUSE frames 	No	No	Yes	Yes	Yes
System time using a Simple Network Time Protocol (SNTP) server or local system counter	Yes	Yes	Yes	Yes	Yes
User-configurable scheduler profile	No	No	Yes	Yes	Yes
User-configurable buffer profile	No	No	Yes	Yes	Yes
Virtual Cable Testing (VCT) technology	Not on third generation modules	Yes	Yes	No	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 4.

Table 4 Supported Layer 2 features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
802.1D Spanning Tree Support: <ul style="list-style-type: none"> 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	ICX 6450 only
802.1p Quality of Service (QoS): <ul style="list-style-type: none"> Strict Priority (SP) Weighted Round Robin (WRR) Combined SP and WRR 8 priority queues 	Yes	Yes	Yes	Yes	Yes
802.1s Multiple Spanning Tree	Yes	Yes	Yes	Yes	Yes
802.1W Rapid Spanning Tree (RSTP)	Yes	Yes	Yes	Yes	Yes
802.3ad link aggregation (dynamic trunk groups)	Yes	Yes	Yes	Yes	Yes
ACL-based rate limiting QoS	Yes	Yes	Yes	Yes	Yes
BPDU Guard	Yes	Yes	Yes	Yes	Yes
Dynamic Host Configuration Protocol (DHCP) Assist	Yes	Yes	Yes	Yes	Yes
IGMP v1/v2 Snooping Global	Yes	Yes	Yes	Yes	Yes
IGMP v3 Snooping Global	Yes (*,G)	Yes (S,G)	Yes (S,G)	Yes (S,G)	Yes
IGMP v1/v2/v3 Snooping per VLAN	Yes	Yes	Yes	Yes	Yes
IGMP v2/v3 Fast Leave (membership tracking)	Yes	Yes	Yes	Yes	Yes
Interpacket Gap (IPG) adjustment	Yes	Yes	Yes	Yes	Yes
IP MTU (individual port setting)	Yes	No	Yes	Yes	ICX 6450 only

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
Jumbo frames: <ul style="list-style-type: none"> Up to 10240 bytes, or Up to 10232 bytes in an IronStack 	Yes	Yes	Yes	Yes	Yes
Link Aggregation Control Protocol (LACP)	Yes	Yes	Yes	Yes	Yes
Link Fault Signaling (LFS) for 10G	Yes	Yes	Yes	Yes	ICX 6450 only
MAC-Based VLANs, including support for dynamic MAC-Based VLAN activation	No	Yes	Yes	Yes	Yes
Metro Ring Protocol 1 (MRP 1)	Yes	Yes	Yes	Yes	Yes
Metro Ring Protocol 2 (MRP 2)	Yes	Yes	Yes	Yes	Yes
Multi-chassis Trunking (supported on FSX devices that have the following modules: <ul style="list-style-type: none"> SX-FI-24GPP SX-FI-24HF SX-FI-2XG SX-FI-8XG SX-FI48GPP 	FSX 800 and FSX 1600 only	No	No	No	No
Extended MRP ring IDs from 1 – 1023	Yes	No	Yes	Yes	Yes
MLD Snooping V1/V2: <ul style="list-style-type: none"> MLD V1/V2 snooping (global and local) MLD fast leave for V1 MLD tracking and fast leave for V2 Static MLD and IGMP groups with support for proxy 	Yes	Yes	Yes	Yes	Yes
Multicast static group traffic filtering (for snooping scenarios)	No	Yes	Yes	Yes	Yes
PIM-SM V2 Snooping	Yes	Yes	Yes	Yes	Yes
PVST/PVST+ compatibility	Yes	Yes	Yes	Yes	Yes
PVRST+ compatibility	Yes	Yes	Yes	Yes	Yes
Remote Fault Notification (RFN) for 1 G fiber	Yes	Yes	Yes	Yes	No
Root Guard	Yes	Yes	Yes	Yes	Yes
Single link LACP	Yes	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
Super Aggregated VLANs	Yes	Yes	Yes	Yes	Yes
Trunk groups: <ul style="list-style-type: none"> Trunk threshold for static trunk groups Flexible trunk group membership Option to include Layer 2 in trunk hash calculation (FWS only) 	Yes	Yes	Yes	Yes	Yes
Topology groups	Yes	Yes	Yes	Yes	Yes
Uni-directional Link Detection (UDLD) (Link keepalive)	Yes	Yes	Yes	Yes	Yes
Uplink Ports within a Port-Based VLAN	Yes	Yes	Yes	Yes	Yes
VLAN Support: <ul style="list-style-type: none"> 4096 maximum VLANs 802.1Q with tagging 802.1ad (Q-in-Q) tagging Dual-mode VLANs GVRP Port-based VLANs Protocol VLANs (AppleTalk, IPv4, dynamic IPv6, and IPX) Layer 3 Subnet VLANs (Appletalk, IP subnet network, and IPX) VLAN groups Private VLANs Multi-range VLANs 	Yes	Yes	Yes	Yes	ICX 6450 uses hardware forwarding, while ICX 6430 uses software forwarding for private VLANs.
VLAN-based mirroring	Yes Supported on 3rd Generation SX modules.	Yes	Yes	Yes	Yes
VoIP Autoconfiguration and CDP	Yes	Yes	Yes	Yes	Yes
Virtual Switch Redundancy Protocol (VSRP)	Yes	Yes	Yes	Yes	Yes
VSRP-Aware security features	Yes	Yes	Yes	Yes	Yes
VSRP and MRP signaling	Yes	Yes	Yes	Yes	Yes
VSRP Fast Start	Yes	Yes	Yes	Yes	Yes
VSRP timer scaling	Yes	Yes	Yes	Yes	Yes

Supported base Layer 3 features

Base Layer 3 software images include all of the management, security, system, and Layer 2 features listed in the previous tables, plus the features listed in Table 5.

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. ICX 6430 devices do not support Layer 3 features..

Table 5 Supported base Layer 3 features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6450
BootP/DHCP Relay	Yes	Yes	Yes	Yes	Yes
Equal Cost Multi Path (ECMP) load sharing	Yes	Yes	Yes	Yes	Yes
IP helper	Yes	Yes	Yes	Yes	Yes
RIP V1 and V2 (advertising only)	Yes	Yes	Yes	Yes	Yes
Routing for directly connected IP subnets	Yes	Yes	Yes	Yes	Yes
Static IP routing	Yes	Yes	Yes	Yes	Yes
Virtual Interfaces (up to 512)	Yes	Yes	Yes	Yes	Yes (up to 255)
Virtual Router Redundancy Protocol (VRRP)	Yes	Yes	Yes	Yes	Yes
VRRP timer scaling	Yes	Yes	Yes	Yes	Yes

Supported edge Layer 3 features

Edge Layer 3 software images include all of the management, security, system, Layer 2, and base Layer 3 features listed in the previous tables, plus the features shown in Table 6.

NOTE: Edge Layer 3 images are supported in the FastIron (hardware) models listed in Table 6. These features are also supported with software-based licensing. For details, refer to the chapter “Software-based Licensing” in the *FastIron Configuration Guide*.

Table 6 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 7.

NOTE: Full Layer 3 features are supported in the FastIron (hardware) models listed in Table 7. These features are also supported with software-based licensing. For details, refer to the chapter “Software-based Licensing” in the *FastIron Configuration Guide*.

Table 7 Supported full Layer 3 features

Category and description	FESX-PREM FSX 800-PREM FSX 1600-PREM	FCX	ICX 6610	ICX 6450
Active host routes	Yes (6,000 1st and 2nd Gen modules) 16,000 (3rd Gen modules)	Yes (16,000)	Yes (16,000)	No
Anycast RP	Yes	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)	No
BGP4	Yes	Yes (ADV models)	Yes (ADV models)	No
Distance Vector Multicast Routing Protocol (DVMRP) V2 (RFC 1075)	Yes	No	No	No
Internet Group Management Protocol (IGMP) V1, V2, and V3 (for multicast routing scenarios)	Yes	Yes	Yes	No
ICMP Redirect messages	Yes	Yes	Yes	Yes
IGMP V3 fast leave (for routing)	Yes	Yes	Yes	No
IPv4 point-to-point GRE IP tunnels	Yes (IPv6 devices only and 3 rd gen modules)	Yes	No	No
IPv6 Layer 3 forwarding ¹	Yes	Yes	Yes	No
IPv6 over IPv4 tunnels in hardware ¹	Yes	Yes	Yes	No

Category and description	FESX-PREM FSX 800-PREM FSX 1600-PREM	FCX	ICX 6610	ICX 6450
IPv6 Redistribution ¹	Yes	Yes	Yes	No
IPv6 Static Routes ¹	Yes	Yes	Yes	Yes
Multiprotocol Source Discovery Protocol (MSDP)	Yes	Yes	No	No
OSPF graceful restart	Yes (FSX 800 and FSX 1600 only)	Yes	Yes	Yes
OSPF V2	Yes	Yes	Yes	Yes
OSPF V3 (IPv6) ¹	Yes	Yes	Yes	No
Protocol Independent Multicast Dense mode (PIM-DM) V1 (draft-ietf-pim-dm-05) and V2 (draft-ietf-pim-v2-dm-03)	Yes	Yes	Yes	No
Protocol Independent Multicast Sparse mode (PIM-SM) V2 (RFC 2362)	Yes	Yes	Yes	No
PIM passive	Yes	Yes	Yes	No
Policy-Based Routing (PBR)	Yes	Yes	Yes	No
RIPng (IPv6) ¹	Yes	Yes	Yes	No
Route-only support (Global CONFIG level and Interface level)	Yes	Yes	Yes	Yes
Route redistribution (including BGP4)	Yes	Yes (BGP4 supported on ADV models only)	Yes (BGP4 supported on ADV models only)	Yes. (BGP4 not supported)
Routes in hardware maximum: <ul style="list-style-type: none"> 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	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	ICX 6450
Static ARP entries	Yes (up to 6,000)	Yes (up to 1,000)	Yes (up to 1,000)	Yes
VRRP-E	Yes	Yes	Yes	Yes
VRRP-E slow start timer	Yes	Yes	Yes	Yes
VRRP-E timer scale	Yes	Yes	Yes	Yes

Supported IPv6 management features

Table 8 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 8 Supported IPv6 management features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
Link-Local IPv6 Address	Yes	Yes	Yes	Yes	Yes
IPv6 Access List (management ACLs)	Yes	Yes	Yes	Yes	Yes
IPv6 copy	Yes	Yes	Yes	Yes	Yes
IPv6 ncopy	Yes	Yes	Yes	Yes	Yes
IPv6 debug	Yes	Yes	Yes	Yes	Yes
IPv6 ping	Yes	Yes	Yes	Yes	Yes
IPv6 traceroute	Yes	Yes	Yes	Yes	Yes
DNS server name resolution	Yes	Yes	Yes	Yes	Yes
HTTP/HTTPS	Yes	Yes	Yes	Yes	Yes
Logging (Syslog)	Yes	Yes	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes	Yes
SCP	Yes	Yes	Yes	Yes	Yes
SSH	Yes	Yes	Yes	Yes	Yes
SNMP	Yes	Yes	Yes	Yes	Yes
SNMP traps	Yes	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610	ICX 6430 ICX 6450
SNTP	Yes	Yes	Yes	Yes	Yes
TACACS/TACACS+	Yes	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes	Yes

Unsupported features

Table 9 lists the features that are not supported on the FastIron devices. If required, these features are available on other Brocade devices.

Table 9 Unsupported features

System-level features not supported
<ul style="list-style-type: none"> ACL logging of permitted packets
<ul style="list-style-type: none"> Broadcast and multicast MAC filters
<ul style="list-style-type: none"> Outbound ACLs on FWS, and 1st or 2nd generation of FSX modules.
Layer 2 features not supported
<ul style="list-style-type: none"> SuperSpan
<ul style="list-style-type: none"> VLAN-based priority
Layer 3 features not supported
<ul style="list-style-type: none"> AppleTalk routing
<ul style="list-style-type: none"> Foundry Standby Router Protocol (FSRP)
<ul style="list-style-type: none"> IPv6 Multicast Routing
<ul style="list-style-type: none"> IPX routing
<ul style="list-style-type: none"> IS-IS
<ul style="list-style-type: none"> Multiprotocol Border Gateway Protocol (MBGP)
<ul style="list-style-type: none"> Multiprotocol Label Switching (MPLS)
<ul style="list-style-type: none"> Network Address Translation (NAT)

Turbolron 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 Turbolron 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 Turbolron
802.1X accounting	No
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 SNMP packets	No
DHCP Client-Based Auto-Configuration	No
DHCP Server	No
Disabling TFTP Access	Yes
Brocade Network Advisor 11.2.1	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

Supported Management Features Category, Description, and Configuration Notes	Supported on Turboliron
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 Turboliron
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
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 Turbolron
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
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

Supported Security Features Category, Description, and Configuration Notes	Supported on Turbolron
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 Turbolron
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 ACL-based fixed and adaptive rate limiting on inbound ports	Yes
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

Supported System –Level Features Category, Description, and Configuration Notes	Supported on Turbolron
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
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

Supported System –Level Features Category, Description, and Configuration Notes	Supported on Turbolron
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 Turbolron
802.1D Spanning Tree Support Enhanced IronSpan support includes Fast Port Span and Single-instance Span Turbolron switches support up to 255 spanning tree instances for VLANs.	Yes
802.1p Quality of Service (QoS) Strict Priority (SP) Weighted Round Robin (WRR) Combined SP and WRR 8 priority queues	Yes
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	Yes

Supported Layer 2 Features Category, Description, and Configuration Notes	Supported on Turbolron
LACP trunk group ports follow the same configuration rules as for statically configured trunk group ports. Support for single link LACP	
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
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 Turbolron Devices: 4096 maximum VLANs Dual-mode VLANs 802.1Q with tagging Port-based VLANs VLAN groups Private VLANs	Yes

Supported Layer 2 Features Category, Description, and Configuration Notes	Supported on Turbolron
VLAN Q-in-Q 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 Turbolron
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 Static RIP support only. The Brocade device with the base Layer 3 does not learn RIP routes from other Layer 3 devices. However, the device does advertise directly connected routes.	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

Supported Layer 3 Features Category, Description, and Configuration Notes	Supported on Turbolron
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, FESX6, FWS, FCX, and ICX

Important notes about upgrading the software

- FSX and FCX devices can store two Full Layer 3 image or two Layer 2 or Base Layer 3 images.
- ICX 6430 devices can hold two Layer 2 images; ICX 6450 devices can hold two Layer 2 or Layer 3 images.
- FESX6 can store one Full Layer 3 image or two Layer 2 or Base Layer 3 images.
- The image for Release 07.2.00a 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 Release 07.2.00 or earlier to Release 07.4.00 and later, 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: On FCX, ICX 6610, ICX 6430, and ICX 6450 devices, the auto image upgrade feature in Release 07.4.00 and later releases will automatically update the software image on member units when an image mismatch occurs.

Important notes about downgrading the software

- FCX-F devices require software release 06.1.00 or later.
- If software-based licensing is in effect on the device and the software is downgraded to pre-release 07.1.00, software-based licensing will not be supported.
- If FCX units in an IronStack are downgraded from software release 07.4.00 and later to release 06.0.00, in some instances, the units may not be able to form a stack. This will occur if there is a mismatch of BGP capability within the stack (i.e., some units support it and others do not). If you encounter this problem, contact Brocade Technical Support for assistance.
- For FCX units, the 10G module name differs in software releases 07.4.00 and later compared to releases 07.0.01b and 07.0.01c. Therefore, if an FCX is downgraded from software releases 07.4.00 and later to release 07.0.01b or 07.0.01c, the stacking port configuration will be lost and the unit will not be able to join the stack.

Standard upgrade procedure

Before upgrading the software on the device, first read the [Important notes about upgrading the software](#) section.

Software image file for Release 07.4.00p

Table 10 lists the software image file that is available for Release 07.4.00p.

Table 10 Software image file

Device	Boot Image	Flash Image
FESX6 FSX 800 FSX 1600	sxz07401.bin	SXS07400p.bin (Layer 2) or SXL07400p.bin (base Layer 3) or SXR07400p.bin (full Layer 3)
FWS	fgz05000.bin	FWS07400p.bin (Layer 2) or FWSL07400p.bin (base Layer 3) or

Device	Boot Image	Flash Image
		FWSR07400p.bin (edge Layer 3)
FCX ICX 6610	grz07302.bin	FCXS07400p.bin (Layer 2) or FCXR07400p.bin (Layer 3)
ICX 6430 ICX 6450	kxz07401.bin	ICX64S07400p.bin (Layer 2) or ICX64R07400p.bin (Layer 3)
TI 24X	trz07300.bin	TIS07400p.bin (Layer 2) or TIR07400p.bin (Layer 3)

PoE Firmware files

Table 11 lists the PoE firmware file types supported. 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 112 PoE Firmware files

Device	Firmware version	Filename
FESX6 FSX 800 FSX 1600	6.0.6	fsx_poe_06.0.6.fw
FSX 800 with SX-FI648PP or SX-FI-24GPP module FSX 1600 with SX-FI648PP or SX-FI-24GPP module	2.1.0	fsx_poeplus_02.1.0.fw
FCX ICX 6610	2.1.0	fcx_poeplus_02.1.0.fw
ICX 6430 ICX 6450	2.1.0	icx64xx_poeplus_02.1.0.fw

Upgrading the boot code

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 FCS or SX device, you must delete the primary and secondary image
3. Copy the boot code from the TFTP server into flash memory. To do so, enter a command such as the following at the Privileged EXEC level of the CLI.

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

You should see output similar to the following.

FSX, FCX, and ICX 6610 devices:

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

ICX 6430 and ICX 6450 devices:

```
Device#Load to buffer (8192 bytes per dot)
.....
.....
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT...
.....
.....
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. Make sure that the TFTP server and the image file are reachable before deleting the image from flash.

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 a 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.

FSX, FCX, and ICX 6610 devices:

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

ICX 6430 and ICX 6450 devices:

```
Device#Load to buffer (8192 bytes per dot)
.....
.....
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT...
.....
.....
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: ICX 6430 and 6450 units can not co-exist in the same stack.

When upgrading the flash image version, the image is automatically updated across all stack units. For other devices, 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 in the IronStack 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) 1996-2012 Brocade Communications Systems, Inc. All rights reserved.
```

```
UNIT 5: compiled on Feb  1 2012 at 12:53:33 labeled as ICX64R07400  
(12475148 bytes) from Primary ICX64R07400.bin
```

```
SW: Version 07.4.00b1T313
```

```
UNIT 1: compiled on Feb  1 2012 at 12:53:33 labeled as ICX64R07400  
(12475148 bytes) from Primary ICX64R07400.bin
```

```
SW: Version 07.4.00b1T313
```

```
UNIT 2: compiled on Feb  1 2012 at 12:53:33 labeled as ICX64R07400  
(12475148 bytes) from Primary ICX64R07400.bin
```

```
SW: Version 07.4.00b1T313
```

```
UNIT 3: compiled on Feb  1 2012 at 12:53:33 labeled as ICX64R07400  
(12475148 bytes) from Primary ICX64R07400.bin
```

```
SW: Version 07.4.00b1T313
```

```
UNIT 4: compiled on Feb  1 2012 at 12:53:33 labeled as ICX64R07400  
(12475148 bytes) from Primary ICX64R07400.bin
```

```
SW: Version 07.4.00b1T313
```

```
UNIT 6: compiled on Feb  1 2012 at 12:53:33 labeled as ICX64R07400  
(12475148 bytes) from Primary ICX64R07400.bin
```

```
SW: Version 07.4.00b1T313
```

```
UNIT 7: compiled on Feb  1 2012 at 12:53:33 labeled as ICX64R07400  
(12475148 bytes) from Primary ICX64R07400.bin
```

```
SW: Version 07.4.00b1T313
```

```
Boot-Monitor Image size = 774984, Version:07.4.00T310 (kxz07400)
```

```
HW: Stackable ICX6450-24-HPOE
```

```
=====
UNIT 1: SL 1: ICX6450-24p POE 24-port Management Module
        Serial #: CEW0451G00W
        License: ICX6450_PREM_ROUTER_SOFT_PACKAGE (LID: egyFJKGiFFy)
        P-ENGINE 0: type DEF0, rev 01
=====
```

```
UNIT 1: SL 2: ICX6450-SFP-Plus 4port 40G Module
=====
```

```
UNIT 2: SL 1: ICX6450-24 24-port Management Module
        Serial #: BZS0442G012
        License: ICX6450_PREM_ROUTER_SOFT_PACKAGE (LID: dbuFJJHiFGH)
        P-ENGINE 0: type DEF0, rev 01
=====
```

```
UNIT 2: SL 2: ICX6450-SFP-Plus 4port 40G Module
=====
```

```
UNIT 3: SL 1: ICX6450-24 24-port Management Module
        Serial #: CEX0451G00F
        License: ICX6450_PREM_ROUTER_SOFT_PACKAGE (LID: egzFJKGiFFh)
        P-ENGINE 0: type DEF0, rev 01
=====
```

```
UNIT 3: SL 2: ICX6450-SFP-Plus 4port 40G Module
=====
```

```
UNIT 4: SL 1: ICX6450-24 24-port Management Module
        Serial #: CEX0451G00E
        License: ICX6450_PREM_ROUTER_SOFT_PACKAGE (LID: egzFJKGiFFg)
```

```

P-ENGINE 0: type DEF0, rev 01
=====
UNIT 4: SL 2: ICX6450-SFP-Plus 4port 40G Module
=====
UNIT 5: SL 1: ICX6450-24p POE 24-port Management Module
      Serial #: BZR0442G00R
      License: ICX6450_PREM_ROUTER_SOFT_PACKAGE (LID: dbtFJJHiFFt)
      P-ENGINE 0: type DEF0, rev 01
=====
UNIT 5: SL 2: ICX6450-SFP-Plus 4port 40G Module
=====
UNIT 6: SL 1: ICX6450-48p POE 48-port Management Module
      Serial #: BZT0442G00Y
      License: ICX6450_PREM_ROUTER_SOFT_PACKAGE (LID: dbvFJJHiFFa)
      P-ENGINE 0: type DEF0, rev 01
      P-ENGINE 1: type DEF0, rev 01
=====
UNIT 6: SL 2: ICX6450-SFP-Plus 4port 40G Module
=====
UNIT 7: SL 1: ICX6450-48p POE 48-port Management Module
      Serial #: BZT0442G01L
      License: ICX6450_PREM_ROUTER_SOFT_PACKAGE (LID: dbvFJJHiFGn)
      P-ENGINE 0: type DEF0, rev 01
      P-ENGINE 1: type DEF0, rev 01
=====
UNIT 7: SL 2: ICX6450-SFP-Plus 4port 40G Module
=====

```

Troubleshooting a failed software image installation

If the software installation fails, the switch might reboot continuously. Do the following to recover from a failed image installation:

1. Enter “b” to interrupt the reload and enter the boot loader prompt.
2. Boot from the other partition. If your software installation was to the primary partition, you can boot from the other partition, which was unaffected. Enter the following command at the boot loader prompt:

```
ICX64XX-boot>>boot_secondary
```

Or

```
ICX64XX-boot>>boot_primary
```

Upgrading software for Turbolron 24X

Use the procedures in this section to upgrade the software on Turbolron 24X.

Factory Pre-loaded Software

This table lists the software that is factory-loaded into the primary and secondary flash areas on the device. All images are included on the CD-ROM shipped with the device.

Model	Software Images	
	Primary Flash	Secondary Flash

Turbolron 24X Series	Layer 2	Layer 3
----------------------	---------	---------

Note: Download the Layer 3 image, from my.brocade.com.

Upgrading software images

Upgrading the Boot Code

1. Place the new boot code on a TFTP server to which the device has access.
2. Enter the following command at the Privileged EXEC level of the CLI (example: FastIron Switch#) to copy the boot code from the TFTP server into flash memory:
copy tftp flash <ip-addr> <image-file-name> bootrom
3. Use the **copy tftp flash** command to copy the boot code to the Brocade device only during a maintenance window. Attempting to do so during normal networking operations can 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
5. The output will display the compressed boot ROM code size and the boot code version.
6. Upgrade the flash code as instructed in the following section.

Upgrading the Flash Code

1. Place the new flash code on a TFTP server to which the Brocade device has access.
2. Enter the following command at the Privileged EXEC level of the CLI (example: FastIron#) to copy the flash code from the TFTP server into the flash memory:
copy tftp flash <ip-addr> <image-file-name> primary | secondary
3. Verify that the flash code has been successfully copied by entering the following command at any level of the CLI:
show flash
4. If the flash code version is correct, go to Step 5. Otherwise, go to Step 1.
5. Reload the software by entering the following command:
reload

(The **reload** command boots from the default boot source, which is the primary flash area by default)

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
<i>FastIron Configuration Guide</i>	Provides configuration procedures for system-level features, enterprise routing protocols, and security features.
<i>Brocade FCX Series Hardware Installation Guide</i> <i>Brocade FastIron WS Hardware Installation Guide</i> <i>Brocade FastIron SX Series Chassis Hardware Installation Guide</i> <i>Brocade FastIron Edge X-Series Switch Hardware Installation guide</i> <i>Brocade ICX 6610 Stackable Switch Hardware Installation Guide</i> <i>Brocade ICX 6450, ICX 6430 Switch Hardware Installation Guide</i>	Describes the hardware as shipped. Provides installation instructions, hardware maintenance procedures, hardware specifications, and compliance information.
<i>Unified IP MIB Reference</i>	Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.
<i>Brocade FCX, Brocade FastIron SX, Brocade ICX Web Management Interface User Guide</i>	Describes the Graphical User Interface (GUI) and procedures for monitoring and configuring various features of the FastIron CX series switches using the GUI.
<i>TurboIron 24X Configuration Guide</i>	Provides configuration procedures for system-level features, enterprise routing protocols, and security features for TurboIron 24X.
<i>Brocade TurboIron 24X Series Hardware Installation Guide</i>	Describes the TurboIron 24X hardware as shipped. Provides installation instructions, hardware maintenance procedures, hardware specifications, and compliance information.
<i>Brocade FastIron, FCX, ICX, and TurboIron Diagnostic Reference</i>	

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

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

Customer reported defects closed with code in Release 07.4.00p

Defect ID: DEFECT000587494	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.30	Technology: LLDP - Link Layer Discovery Protocol
Symptom: FI device may unexpectedly reload when plugging/unplugging phone by LLDP.	
Condition: This issue may occur on FI device connected to a phone with LLDP	
Workaround: Remove "lldp enable snmp med-topo-change-notifications ports" configuration	

Defect ID: DEFECT000589112	
Technical Severity: Medium	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 07.4.00	Technology: Software Installation & Upgrade
Symptom: In SX800 device with 48GC PUMA line cards, sometimes the cards fail to initialize.	
Condition: When upgrading from 7.3p to 7.4j image, 48GC PUMA line cards in SX800 cards fail to initialize.	

Customer reported defects closed with code in Release 07.4.00n

Defect ID: DEFECT000557199	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Monitoring
Reported In Release: FI 07.4.00	Technology: Hardware Monitoring
Symptom: In the 2 unit ICX6450 stack, the standby unit reloads randomly.	
Condition: When Jumbo is enabled, SDMA is stuck with higher MTU which causes the Watchdog to be kicked in and thus the reload of standby unit.	

Defect ID: DEFECT000562355	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: FI 07.3.00	Technology: IP Addressing
Symptom: In FWS device, software forwarding for the unicast traffic results in high CPU.	
Condition: With 'ip-subnet vlan' configured, the high CPU is observed when software forwarding for the unicast traffic happens.	

Defect ID: DEFECT000581402	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: FI 07.3.00	Technology: Static Routing (IPv4)
Symptom: In SX800 device, routing loop will be observed.	
Condition: When SX800 is running with 7.3p or 7.4m code, the routing loop will be observed since the default route learned through OSPF is used instead of more specific static route.	

Customer reported defects closed with code in Release 07.4.00m

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

Defect ID: DEFECT000564926	
Technical Severity: Medium	Probability: Medium
Product: Brocade FastIron OS	Technology: Security
Reported In Release: FI 07.2.02	Technology Area: HTTP/HTTPS
Symptom: Memory leak on FI device.	
Condition: This issue can be seen in FI device when HTTPs is enabled.	
Recovery: Reload of device.	

Defect ID: DEFECT000567600	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology: Security
Reported In Release: FI 07.4.00	Technology Area: SSH – Secure Shell
Symptom: Device with low or out of memory due to leak in SSH	
Condition: This issue can be seen with the device running firmware version FI 7.4.00 or later and frequent SSH logins and logouts.	

Customer reported defects closed with code in Release 07.4.00k

Defect ID: DEFECT000441699	
Technical Severity: Medium	Probability: Medium
Product: Brocade FastIron	Technology: Security
Reported In Release: FI 08.0.00	Technology Area: HTTP/HTTPS
Symptom: FrontPanel is not launched with the certificate generated using MD5.	
Condition: This issue can be seen with latest BNA which does not support the weaker cipher algorithms like MD5 and HTTPS configured in the device.	

Defect ID: DEFECT000555431	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron	Technology: Management
Reported In Release: FI 08.0.10	Technology Area: Configuration Fundamentals
Symptom: The port transitions and incrementing InErrors are seen on 10G ports of ICX6450-24.	
Condition: When Jumbo frames is enabled in ICX6450-24, the port transitions and incrementing InErrors are seen on 10G ports of ICX6450-24.	

Defect ID: DEFECT000560547	
Technical Severity: High	Probability: Low
Product: Brocade FastIron	Technology: Management
Reported In Release: FI 07.4.00	Technology Area: Configuration Fundamentals
Symptom: FastIron SuperX / SX will reload continuously on software upgrade from 7.4d to 7.4j.	
Condition: When doing software upgrade from 7.4d to 7.4j, boot loop will be observed in FastIron SuperX / SX.	

Defect ID: DEFECT000561940	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron	Technology: Management
Reported In Release: FI 07.3.00	Technology Area: Configuration Fundamentals
Symptom: The port transitions and incrementing InErrors are seen on 10G ports of ICX6450-24.	
Condition: When Jumbo frames is enabled in ICX6450-24, the port transitions and incrementing InErrors are seen on 10G ports of ICX6450-24.	

Defect ID: DEFECT000562313	
Technical Severity: Medium	Probability: High
Product: Brocade FastIron	Technology: Layer 2 Switching
Reported In Release: FI 07.3.00	Technology Area: VLAN - Virtual LAN
Symptom: ICX6610 device may unexpectedly reload when adding up link ports to VLAN before configuring member ports.	
Condition: This issue is seen on addition of uplink ports to the VLAN before configuring member ports.	

Defect ID: DEFECT000562729	
Technical Severity: Medium	Probability: High
Product: Brocade FastIron	Technology: Other
Reported In Release: FI 07.4.00	Technology Area: Other
Symptom: In FI 7.4.00, "show media" on SFP and SFP+ transceivers are not displayed correctly.	
Condition: Collect "sh media" information on SFP and SFP+ transceivers.	

Defect ID: DEFECT000565895	
Technical Severity: Critical	Probability: Low
Product: Brocade FastIron	Technology: Stacking
Reported In Release: FI 07.4.00	Technology Area: Traditional Stacking
Symptom: The standby unit in stack may unexpectedly reload during image sync.	
Condition: This issue may occur during image sync in member/standby unit.	

Defect ID: DEFECT000566388	
Technical Severity: High	Probability: Low
Product: Brocade FastIron	Technology: Stacking
Reported In Release: FI 07.4.00	Technology Area: Traditional Stacking
Symptom: ICX6610 may unexpectedly reload	
Condition: This issue may be seen when displaying virtual interfaces in detail using CLI command.	

Defect ID: DEFECT000567117	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron	Technology: Layer 3 Routing/Network Layer
Reported In Release: FI 07.4.00	Technology Area: IP Addressing
Symptom: The device may unexpectedly reload with DHCP snooping enabled.	
Condition: This issue may be seen when the device has many pending ARP entries with DHCP snooping enabled on the device.	
Workaround: Turn off DHCP snooping.	

Customer reported defects closed with code in Release 07.4.00j

Defect ID: DEFECT000460514	
Technical Severity: Medium	Probability: High
Product: IronWare	Technology: System
Reported In Release: FI 07.3.00	Technology Area: Optics
Symptom: In SX800, long ICMP response time and high CPU are observed.	
Condition: When optical-monitoring is enabled, long ICMP response time and high CPU are observed in SX800 devices.	
Workaround: Remove optical monitoring.	

Defect ID: DEFECT000468746	
Technical Severity: High	Probability: High
Product: IronWare	Technology: Layer 2
Reported In Release: FI 08.0.00	Technology Area: IEEE 802.1w RSTP
Symptom: With PVRST mode enabled on the VDX device, the FastIron devices drops BPDUs from the VDX device resulting in non-convergence of the topology.	
Condition: When VDX device with Spanning tree and PVRST mode enabled is connected to a FastIron device, the BPDUs are dropped resulting issue in topology convergence.	

Defect ID: DEFECT000506391	
Technical Severity: Medium	Probability: High
Product: IronWare	Technology: Traffic Management
Reported In Release: FI 07.3.00	Technology Area: QoS - Quality of Service
Symptom: The “egress-buffer-threshold minimum” configuration on LACP/Trunk interface does not take effect on secondary ports after reload.	
Condition: When “egress-buffer-threshold minimum” is configured on LACP / Trunk interfaces, the configuration is shown only on primary interface in the startup configuration. The configuration is not applied on the secondary ports upon reload.	
Recovery: Re-configure the 'egress-buffer-threshold minimum' command after reload	

Defect ID: DEFECT000530578	
Technical Severity: High	Probability: Medium
Product: IronWare	Technology: Layer 3
Reported In Release: FI 07.4.00	Technology Area: Other IPv4
Symptom: IP reachability issues are observed between hosts in specific subnets connected in different VLANs.	
Condition: In SX800, during switch fabric hotswap, the hosts in specific subnets connected in different VLANs are facing IP reachability issues.	

Defect ID: DEFECT000537902	
Technical Severity: High	Probability: Medium
Product: IronWare	Technology: Stacking
Reported In Release: FI 07.3.00	Technology Area: Traditional Stacking
Symptom: ICX6610 stack unit segmented/deleted itself from the stack	
Condition: During operation, the ICX6610 stack unit got segmented/deleted itself from the stack	
Recovery: This is a corner case which was seen sometime. The ICX6610 got segmented from the stack. To recover the problem the affected unit can be reloaded which can re-establish its communication with rest of the stacking units	

Defect ID: DEFECT000538959	
Technical Severity: High	Probability: High
Product: IronWare	Technology: System
Reported In Release: FI 07.4.00	Technology Area: Component
Symptom: Rapid increment of CRC errors seen in 10GB cards in SX devices.	
Condition: CRC errors are seen only on 10GB uplinks between core switches (MCT links) or edge switch uplinks to core switches	
Workaround: Reboot the switch connected to the port on which CRC errors are seen.	

Defect ID: DEFECT000541620	
Technical Severity: High	Probability: High
Product: IronWare	Technology: System
Reported In Release: FI 07.4.00	Technology Area: Component
Symptom: In FastIron SX800 device, the SX-FI-48GPP line cards does not boot/initialize properly at certain instances.	
Condition: When SX-FI-48GPP modules with serial numbers ending in JXXX (fourth from the last character is a "J"), is used on SX800/1600 device, the line cards are not recognized after throwing an	
Recovery: After reloading the chassis on one of the affected code versions, enter "enable module <module-id>" command for the affected module. The module will initialize and run until the chassis is	

Defect ID: DEFECT000543334	
Technical Severity: High	Probability: High
Product: IronWare	Technology: Layer 2
Reported In Release: FI 07.4.00	Technology Area: Link Aggregation
Symptom: LACP stuck in 'Init' state after ICX6610 stack reloaded	
Condition: When LAG is configured on top of SSTP and ICX6610 stack is reloaded.	

Defect ID: DEFECT000544654	
Technical Severity: High	Probability: High
Product: IronWare	Technology: Layer 3
Reported In Release: FI 07.4.00	Technology Area: OSPF (IPv4)
Symptom: Redistribution of static and connected routes were not working in OSPF on running on	
Condition: The issue is observed during redistribution of static and connected routes under OSPFv2. Problem is there only with 7.x.x.x releases.	

Defect ID: DEFECT000545366	
Technical Severity: High	Probability: High
Product: IronWare	Technology: Layer 3
Reported In Release: FI 07.3.00	Technology Area: Other IPv4
Symptom: In FastIron FCX stack device, IP reachability issue is observed on ports connected to the active unit when it is elected through stack priority change.	
Condition: When stack MAC address is configured in the FastIron stack device, and if the active unit gets elected through stack priority change, IP reachability issues are observed on the active units' ports.	

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

Defect ID: DEFECT000553767	
Technical Severity: Medium	Probability: High
Product: IronWare	Technology: Management
Reported In Release: FI 07.4.00	Technology Area: Web Management
Symptom: In ICX6450, dual-mode and router-ve configurations cannot be removed using Web GUI.	
Condition: When removing dual-mode and router-ve configurations in ICX6450 using Web GUI, the configurations are not removed.	

Customer reported defects closed with code in Release 07.4.00h

Defect ID: DEFECT000358890	
Technical Severity: Critical	Probability: High
Product: IronWare	Technology: Management
Reported In Release: FI 07.3.00	Technology Area: SSH - Secure Shell
Symptom: When launching an SSHv2 session after a hitless reload SX1600 may reset.	
Condition: Initiating SSHv2 session after hitless reload on SX1600 may reset the device.	

Defect ID: DEFECT000491231	
Technical Severity: Medium	Probability: High
Product: IronWare	Technology: Management
Reported In Release: FI 07.4.00	Technology Area: SSH - Secure Shell
Symptom: Memory leak is observed in the FastIron device when CLI commands that generates large output are issued on the SSH session, .	
Condition: When commands that generates large output are issued on the SSH session, memory leak is observed in the FastIron device.	

Defect ID: DEFECT000530462	
Technical Severity: Medium	Probability: High
Product: IronWare	Technology: Layer 3
Reported In Release: FI 08.0.01	Technology Area: BGP4 (IPv4)
Symptom: BGP route reflector does not discard a route whose Cluster list contains the route reflector's own cluster ID.	
Condition: The issue occurs whenever a route reflector receives a route with the Cluster list having its own cluster ID.	

Defect ID: DEFECT000532029	
Technical Severity: Critical	Probability: High
Product: IronWare	Technology: Stacking
Reported In Release: FI 07.4.00	Technology Area: Traditional Stacking
Symptom: High CPU is observed on all ICX6450 unites when three or more ICX6450 stack devices are linked to a hub or a VCX device.	
Condition: When ICX6450 stack devices are connected in a “star” topology through a non-stacking VDX device, high CPU is seen in all the ICX units.	
Workaround: Apply ACL on the ingress interface of the hub where the ICX stacks are connected so that the stacking packets leaking into other stacking units through the hub are dropped.	

Defect ID: DEFECT000533382	
Technical Severity: High	Probability: Low
Product: IronWare	Technology: Stacking
Reported In Release: FI 07.2.00	Technology Area: Hitless Switchover, Failover, Hotswap, OS U/G
Symptom: The active management module of SX800 device unexpectedly reloads without stack trace.	
Condition: If the SX800 device is up for more than 1325 days, the active management module resets unexpectedly.	

Defect ID: DEFECT000533770	
Technical Severity: High	Probability: Medium
Product: IronWare	Technology: Management
Reported In Release: FI 07.4.00	Technology Area: DHCP (IPv4)
Symptom: Upon DHCP renewal of clients, ARP is resolved to the non-primary port of trunk instead of primary port in the ICX 6610 device.	
Condition: This issue is observed only when DHCP snooping is configured over a LAG interface.	

Defect ID: DEFECT000533795	
Technical Severity: High	Probability: Medium
Product: IronWare	Technology: Layer 2
Reported In Release: FI 07.4.00	Technology Area: ARP
Symptom: In ICX6610 device, CPU goes high after ARP age out even with continuous traffic	
Condition: After ARP ages out, the packets are trapped to CPU resulting in loading the CPU of the ICX6610 device	

Defect ID: DEFECT000535464	
Technical Severity: Medium	Probability: High
Product: IronWare	Technology: Layer 2
Reported In Release: FI 05.1.00	Technology Area: MAC ACLs
Symptom: IPv6 packets are denied when MAC filter is configured in FESX device.	
Condition: On FESX, upon configuring MAC filter on the interface, IPv6 packets are dropped.	

Defect ID: DEFECT000535762	
Technical Severity: High	Probability: High
Product: IronWare	Technology: Security
Reported In Release: FI 07.4.00	Technology Area: Web Authentication
Symptom: After customer upgraded to 7.4x webauth stop working for users	
Condition: Customer upgraded multiple switches from 07.0.01 to 07.4.00d. "After the upgrade, webauth would no longer work	
Recovery: Customer tried downgrading back to 07.0.01 to recovery with no success.	

Defect ID: DEFECT000536874	
Technical Severity: High	Probability: Low
Product: IronWare	Technology: Management
Reported In Release: FI 07.4.00	Technology Area: DHCP (IPv4)
Symptom: DHCP release messages from DHCP clients are not processed in ICX6610 device.	
Condition: When the ARP ages out for the DHCP client, the DHCP release messages are not processed by ICX6610 device	

Defect ID: DEFECT000537998	
Technical Severity: Medium	Probability: High
Product: IronWare	Technology: Layer 2
Reported In Release: FI 07.4.00	Technology Area: VSRP - Virtual Switch Redundancy Protocol
Symptom: The "restart-vsrp-port 1" command does not persist across reload.	
Condition: When the "restart-vsrp-port 1" command is issued with the default value timer value which is "1", the command is not saved in the configuration.	
Workaround: Configuring VSRP fast restart feature with non-default timer value will not cause this issue.	

Defect ID: DEFECT000539843	
Technical Severity: Critical	Probability: Low
Product: IronWare	Technology: System
Reported In Release: FI 07.4.00	Technology Area: Component
Symptom: The ICX6610 device starts getting InErrors / CRC errors due to SFI link down events detected in PHY after certain period.	
Condition: After running error free for certain period of time (1/2 hour to 3 hours), the ICX6610 device starts getting InErrors / CRC errors due to SFI link down events detected in PHY	

Defect ID: DEFECT000544763	
Technical Severity: High	Probability: Low
Product: IronWare	Technology: Layer 3
Reported In Release: FI 07.4.00	Technology Area: Other IPv4
Symptom: The standby unit of ICX6610 stack device is not accessible after DHCP release/ renew.	
Condition: After DHCP release / renew test, the standby unit of ICX6610 device becomes non-responsive.	

Customer reported defects closed with code in Release 07.4.00g

Defect ID: DEFECT000511114	
Technical Severity: High	Probability: Low
Product: IronWare	Technology: Stacking
Reported In Release: FI 07.4.00	Technology Area: Traditional Stacking
Symptom: On ICX6610 all rconsoles to the master has no response if the master has problem in receiving packet	
Condition: None	

Defect ID: DEFECT000516553	
Technical Severity: Critical	Probability: High
Product: IronWare	Technology: Stacking
Reported In Release: FI 07.4.00	Technology Area: Traditional Stacking
Symptom: In ICX stacking environment, sometimes a member gets isolated from the stack due to a transmit lockup. This is result of inability to transmit packets on the 40G link, causing the member to be removed from the stack.	
Condition: This could be caused due to flapping of the 40G port, or in a congestion situation. The following syslog will show that stack with name XYZ, unit 2 is removed due to transmit lockup: 6/21/2014 10:41:01.566 PM 192.168.10.1 XYZ Stack: Stack unit 2 has been deleted to the stack system	

Defect ID: DEFECT000521957	
Technical Severity: High	Probability: High
Product: IronWare	Technology: IP Multicast
Reported In Release: FI 07.4.00	Technology Area: IPv4 Multicast Switching
Symptom: The Switch does not remove the outgoing interface from multicast forwarding entry when a prune message is received on the interface	
Condition: The defect appears when the first few prune messages are processed in certain order that the Switch enters into a state where it does not remove the oif from the forward entry for a longer duration, and continues to forward multicast traffic.	

Defect ID: DEFECT000523929	
Technical Severity: High	Probability: Low
Product: IronWare	Technology: Stacking
Reported In Release: FI 08.0.20	Technology Area: Traditional Stacking
Symptom: AAA authentication is enabled. The active controller rconsoles to the standby. If the rconsole is terminated by "exit". The following rconsole to the standby will not be in privileged mode and cannot access "dm" and other commands.	
Condition: None.	
Workaround: Workaround: Using <ctrl> o x, not exit, to terminate the rconsole does not cause this problem.	

Defect ID: DEFECT000524539	
Technical Severity: High	Probability: High
Product: IronWare	Technology: IP Multicast
Reported In Release: FI 07.4.00	Technology Area: IPv4 Multicast Switching
Symptom: There is an intermittent loss of multicast traffic when traffic is forwarded through the stacking link of a Stack.	
Condition: This issue is seen when multiple operations are done on an entry, such as addition and removal of port from forwarding entry.	

Defect ID: DEFECT000526892	
Technical Severity: Medium	Probability: Medium
Product: IronWare	Technology: Layer 2
Reported In Release: FI 07.4.00	Technology Area: UDLD - Uni-Directional Link Detection
Symptom: In a Switch/Router configured with UDLD, if a flap is seen, the debug counter can be used to isolate the cause of flap.	
Condition: The UDLD flap could be caused due to either UDLD packet is not received, or it was not sent out.	

Defect ID: DEFECT000527865	
Technical Severity: High	Probability: Low
Product: IronWare	Technology: Stacking
Reported In Release: FI 07.4.00	Technology Area: Traditional Stacking
Symptom: ICX6610 40G port can sometimes flap.	
Condition: In the 40G PHY, spurious internal PHY event can lead to port flap.	

Defect ID: DEFECT000528969	
Technical Severity: High	Probability: Medium
Product: IronWare	Technology: Stacking
Reported In Release: FI 07.4.00	Technology Area: Traditional Stacking
Symptom: Occasionally, the 40G port incurs a microflap for a very short duration that can lead to packet loss	
Condition: Sometimes, a sensitive 40G receiver in presence of noise can cause a microflap.	

Customer reported defects closed with code in Release 07.4.00f

Defect ID: DEFECT000398232	Technical Severity: High
Summary: An unexpected reset is encountered when RSTP cost and edge port are set on a port outside the VLAN through Web Management Interface.	
Symptom: When the Web Management Interface is used to set RSTP cost and edge port on a port that is not currently a member of the selected VLAN, an unexpected reset is experienced.	
Probability: Low	Risk of Fix: Medium
Feature: FI Embedded Management	Function: Web Management
Reported In Release: FI 07.3.00	Service Request ID: 723983

Defect ID: DEFECT000410498	Technical Severity: Medium
Summary: First VLAN IP subnet name is erased when protocol "xxx-proto" is configured in the VLAN. The dynamic IPv6 protocol VLAN membership that is disabled (using the "ipv6-proto" and no dynamic) is enabled after a reboot in router.	
Symptom: First VLAN IP subnet name is erased after reload.	
Probability: Medium	Risk of Fix: Medium
Feature: SX L2 Forwarding	Function: Protocol VLAN
Reported In Release: FI 07.2.02	Service Request ID: 751033

Defect ID: DEFECT000413089	Technical Severity: Medium
Summary: In ICX, layer1 interface status comes up before the boot process of the other end of the connected device is completed.	
Symptom: When two ICX6610 devices are connected each other, the connected interface at local device shows Layer 1 as up before the other end completely reboots.	
Probability: Low	
Feature: Platform	Function: System
Reported In Release: FI 07.4.00	Service Request ID: 738385

Defect ID: DEFECT000426210	Technical Severity: Medium
Summary: When TACACS+ is configured, issuing any "dm" command makes the CLI unresponsive until the carriage return is pressed	
Symptom: When TACACS+ is configured, issuing any "dm" command makes the CLI unresponsive until the carriage return is pressed, and may cause problems with scripted data collection.	
Probability: High	
Feature: FI Embedded Management	Function: CLI Parser
Reported In Release: FI 07.4.00	Service Request ID: 1101096

Defect ID: DEFECT000456070	Technical Severity: Medium
Summary: The "show fdp neighbor" command output displays only 14 characters instead of 17 characters.	
Symptom: The "show fdp neighbor" command output displays only 14 characters, whereas the "show cdp neighbor" command output displays 17 characters. So, the customer cannot identify the host name of the connected third party phones.	
Probability: High	Risk of Fix: Low
Feature: SX L2 Control	Function: FDP and CDP(VOIP autoconfiguration)
Reported In Release: FI 07.3.00	Service Request ID: 1154085

Defect ID: DEFECT000470564	Technical Severity: Medium
Summary: When “ip mroute 1 0.0.0.0 0.0.0.0 rpf_address <ip address>” is configured, the command takes effect but the route does not appear in the “show ip mroute” output.	
Symptom: "show ip mroute" does not display a configured static default multicast route in the output.	
Probability: Medium	Risk of Fix: Low
Feature: SX L2/L3 Multicast Features	Function: PIM Sparse
Reported In Release: FI 07.3.00	Service Request ID: 1210623

Defect ID: DEFECT000471141	Technical Severity: Medium
Summary: ICX device floods flow control packets without any 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.	
Probability: High	Risk of Fix: Low
Feature: FI Infrastructure	Function: qos unknown
Reported In Release: FI 08.0.01	Service Request ID: 724451

Defect ID: DEFECT000471565	Technical Severity: Medium
Summary: An SCP file transfer using Putty version 0.63 over a slow connection may fail.	
Symptom: An SCP file transfer using Putty version 0.63 over a slow connection may fail and generate the following error message: Fatal: Received unexpected end-of-file from server.	
Probability: Medium	Risk of Fix: Medium
Feature: FI Embedded Management	Function: SSHV2/SCP
Reported In Release: FI 07.3.00	Service Request ID: 1213955,1213955

Defect ID: DEFECT000471814	Technical Severity: Medium
Summary: Stacking power supply table OID does not work for all stack units	
Symptom: The power supply module status for all stack member units is not displayed when the OID snChasPwrSupply2Table is polled.	
Probability: Medium	Risk of Fix: Low
Feature: FI Embedded Management	Function: SNMP v1/v2/v3
Reported In Release: FI 07.3.00	Service Request ID: 1204770,1231835

Defect ID: DEFECT000473539	Technical Severity: Medium
Summary: "admin-pt2pt-mac" configuration automatically gets added at VLAN level after a system reload	
Symptom: If "spanning-tree 802 admin-pt2pt-mac" command is added at interface configuration level and saved to the configuration, upon reloading the system, "spanning-tree 802-1w ethe <port-num> admin-pt2pt-mac" appears at the VLAN configuration level.	
Probability: High	Risk of Fix: Low
Feature: FCX L2 Control	Function: 802.1w
Reported In Release: FI 07.3.00	Service Request ID: 1222349

Defect ID: DEFECT000473755	Technical Severity: Medium
Summary: SNMP tells that power supply is down, but works well	
Symptom: SNMP tells that power supply is down, but works well	
	Risk of Fix: Low
Feature: FCX Network Management	Function: SNMP V4/V6
Reported In Release: FI 07.2.02	Service Request ID: 1208707

Defect ID: DEFECT000473881	Technical Severity: Medium
Summary: Reload schedule takes different time in ICX6450-24P.	
Symptom: The "reload after" command does not register the time correctly in some cases. For example, it treats "reload after 00:09:50" as "reload after 00:00:50". Also the "reload after" command does not notify the reload schedule.	
Probability: Medium	
Feature: Platform	Function: System
Reported In Release: FI 07.4.00	Service Request ID: 1225749

Defect ID: DEFECT000478208	Technical Severity: Medium
Summary: Power supply down on standby.	
Symptom: The local log displays the following message at boot up: "Redundant power supply is down".	
Probability: Medium	
Feature: FI Embedded Management	Function: SYSLOG
Reported In Release: FI 07.4.00	Service Request ID: 1239282

Defect ID: DEFECT000481563	Technical Severity: Medium
Summary: BNA cannot access command line interface of an FCX device running 07.4.00d software.	
Symptom: Cannot connect to the CLI of an FCX device running 7.4.00d software through BNA. However, there is no problem while using telnet from PuTTY or Secure CRT with the same setup.	
Probability: High	
Feature: FI Embedded Management	Function: TELNET
Reported In Release: FI 07.4.00	Service Request ID: 1245785

Defect ID: DEFECT000481686	Technical Severity: Medium
Summary: The scheduled reload command using the image from the secondary flash is not working	
Symptom: Scheduled reload in a stack using the image in the secondary flash is having issues. Customer had three switches in a stack and did a scheduled reload by using the command "reload at 20:00:00 9-19-2013 secondary" but the system rebooted with the image from primary, stack didn't get split up and faced few routing issues. Then customer issued the command boot system flash sec to recover this and everything is working fine.	
Workaround: Then customer issued the command boot system flash sec to recover this and everything is working fine.	
Probability: Low	Risk of Fix: Low
Feature: FI Platform	Function: Boot code/Flash/Kernel
Reported In Release: FI 08.0.00	Service Request ID: 1234188

Defect ID: DEFECT000482452	Technical Severity: Medium
Summary: "admin-edge-port" configuration automatically gets added at VLAN level after LAG is established.	
Symptom: "admin-edge-port" configuration automatically gets added at VLAN level after LAG is established.	
	Risk of Fix: Low
Feature: FI L2	Function: Control Plane - LACP
Reported In Release: FI 07.3.00	Service Request ID: 1249659

Defect ID: DEFECT000483285	Technical Severity: Medium
Summary: 1GE Twinax ports report: “Configured speed 1Gbit, actual none, configured duplex fdx, actual none”. We see this in the CLI and also when the device is asked for media type by way of SNMP	
Symptom: Customer has a network monitoring system that utilizes the speed and duplex reports based on our switch to pull data such as bandwidth utilization or port status on those stack ports. He found that some of his stacking ports reports: “Configured speed 1Gbit, actual none, configured duplex fdx, actual none”	
Workaround: This is a display issue.	
Probability: Medium	
Feature: Platform	Function: 1G Link
Reported In Release: FI 07.4.00	Service Request ID: 1251003

Defect ID: DEFECT000485242	Technical Severity: Critical
Summary: when several switch connect to a multi-access section (Hub), running 802.1d or PVST, TCN will not terminate.	
Symptom: There are lots of TCN BPDU in the network, and the network does not become stable.	
Workaround: run RSTP instead	
Probability: High	
Feature: FI L2 control	Function: Spanning-tree protocols /PVST+/PVRST+
Reported In Release: FI 07.4.00	Service Request ID: 1256784

Defect ID: DEFECT000485316	Technical Severity: Medium
Summary: FCX Combo Ports generating optical errors for every 3 minutes even when disconnected SFP and the alternate copper port is used.	
Symptom: FCX shows error " RX power warning error slot 1/1/1" for every 3 minutes.	
Workaround: Removed the SFPs on the ports that do not have fiber connected which stopped the errors.	
Probability: Medium	Risk of Fix: Low
Feature: DOM	Function: DOM
Reported In Release: FI 07.2.02	Service Request ID: 1231134,1231134

Defect ID: DEFECT000485619	Technical Severity: High
Summary: Deny ACL does not work when apply to inbound interface on FCX	
Symptom: Customer has an access-list 160 to deny (UDP/TCP 19) and certain DNS (UDP/TCP 53) traffic. When this ACL is being applied to interface e 1/2/1 on FCX648, it does not block traffic as intended.	
Probability: Medium	Risk of Fix: Low
Feature: FI ACL	Function: ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.3.00	Service Request ID: 1256313

Defect ID: DEFECT000485867	Technical Severity: Medium
Summary: An FSX management module switchover removes the 100-fx and optical monitoring configuration.	
Symptom: An FSX management module switchover removes the 100-fx and optical monitoring configuration.	
Probability: Medium	Risk of Fix: Medium
Feature: DOM	Function: DOM
Reported In Release: FI 07.3.00	Service Request ID: 1257391

Defect ID: DEFECT000485935	Technical Severity: Medium
Summary: ICX 6610 fibre ports are showing up during bootup process itself	
Symptom: ICX 6610 is bringing optical port up during booting process itself i.e even before node is completely up.	
Probability: Medium	Risk of Fix: Medium
Feature: Platform	Function: PHY
Reported In Release: FI 08.0.01	Service Request ID: 1257257,1257257

Defect ID: DEFECT000486447	Technical Severity: Medium
Summary: show optic produced no output in 7300g but works in previous versions if downgraded.	
Symptom: No output for show optic for the below specified 10G optic Type : 10G XG-SR(XFP) Vendor: Brocade Version: A Part# : 33011-000 Type : 10G XG-SR(XFP) Vendor: FOUNDRY NETWORKS Version: A Part# : 33011-000	
Probability: High	Risk of Fix: Medium
Feature: DOM	Function: DOM
Reported In Release: FI 07.3.00	Service Request ID: 1253880

Defect ID: DEFECT000486684	Technical Severity: High
Summary: The System resets when "Show tech" command is issued with DHCP snooping configured on LAG ports.	
Symptom: The system resets occasionally when DHCP snooping is configured on the LAG ports. "Show tech" or generating running configuration can cause this system reset.	
Workaround: downgrade to 7400d	
Probability: Medium	Risk of Fix: Medium
Feature: FI - L4/Security	Function: Others
Reported In Release: FI 08.0.01	Service Request ID: 1254213

Defect ID: DEFECT000486788	Technical Severity: High
Summary: DHCP decline messages are getting dropped	
Symptom: DHCP decline messages are getting dropped by DHCP Relay agent (FCX/SX) when DHCP snooping is enabled for a particular VLAN.	
Probability: Medium	Risk of Fix: Medium
Feature: FCX DHCP	Function: Client
Reported In Release: FI 07.2.02	Service Request ID: 1257664

Defect ID: DEFECT000486953	Technical Severity: Medium
Summary: Third party phones have problems connecting with TFTP server, when ICX6450 and ICX6610 are used as DHCP server.	
Symptom: Third party phones have problems connecting with TFTP server, when ICX6450 and ICX6610 are used as DHCP server.	
Probability: Low	
Feature: FI Embedded Management	Function: DHCP IPv4 Client/Server
Reported In Release: FI 07.4.00	Service Request ID: 1257953

Defect ID: DEFECT000487115	Technical Severity: Medium
Summary: The show “qd-share-level “ output and configuration of “qd-share-level” is conflicting on ICX6430 and ICX6450 devices.	
Symptom: The output of show “qd-share-level” and configuration of “qd-share-level” is in conflict on ICX6430 and ICX6450 devices.	
	Risk of Fix: Low
Feature: FI Infrastructure	Function: qos unknown
Reported In Release: FI 08.0.00	Service Request ID: 1260004

Defect ID: DEFECT000488852	Technical Severity: Medium
Summary: When the next hop is changed due to OSPF topology change, the default route entry in hardware is not getting updated	
Symptom: Even though "show ip route" command output shows that the routing table is updated, traffic still goes out from the port based on the previous routing entry, unless the "clear ip route" command is issued.	
Probability: Low	
Feature: Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.4.00	Service Request ID: 1270067

Defect ID: DEFECT000489101	Technical Severity: Medium
Summary: Configuring the tag mode for the ports in VLAN through SNMP MIB is not working	
Symptom: Using snmpset operation to set the port to tagged(1) and untagged(2) is giving the following error. Error in packet. Reason: undoFailed Failed object: SNMPv2-SMI::enterprises.1991.1.1.3.2.6.1.4.<vlan>.<port-snmp-id>	
Probability: Low	Risk of Fix: Medium
Feature: MANAGEMENT	Function: SNMP
Reported In Release: FI 08.0.00	Service Request ID: 1266824

Defect ID: DEFECT000489359	Technical Severity: Medium
Summary: FI Stack device unexpectedly reloads while trying to set/reset “global icmp redirect” through CLI when ECMP path exists.	
Symptom: An ICX 6610 stack unexpectedly reloads when “no ip icmp redirect” command is issued.	
Probability: Medium	
Feature: Layer 3 Forwarding - IPV4	Function: ECMP (IPV4)
Reported In Release: FI 07.4.00	Service Request ID: 1270536

Defect ID: DEFECT000490425	Technical Severity: Medium
Summary: The "no chassis trap-log fan all" command suppresses only the alerts for the active controller, but not the other units in the stack configuration.	
Symptom: Since there are more than 5,000 FCX devices installed, the fan speed alert messages fill up the logs very quickly. When the "no chassis trap-log fan all" command is issued for a stack configuration, it only suppresses the alerts for the active controller, but not the other units.	
Probability: Medium	Risk of Fix: Low
Feature: FCX Network Management	Function: SYSLOG
Reported In Release: FI 07.3.00	Service Request ID: 1275980

Defect ID: DEFECT000490488	Technical Severity: High
Summary: After routing update, there is a routing loop on an FWS device	
Symptom: After changes in OSPF topology, the FWS device mistakenly routes the traffic destined to its directly connected hosts to its default gateway learnt through OSPF which results in routing loop.	
Probability: Medium	
Feature: Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.4.00	Service Request ID: 1214456

Defect ID: DEFECT000490581	Technical Severity: High
Summary: When the FI device is configured with sflow and snmp-server trap source as loop back, the device may reload unexpectedly during add/removal of IP address on virtual ethernet interface	
Symptom: ICX6610 stack unexpectedly reloads when adding and later removing an IP address of the VE interface.	
Probability: Low	Risk of Fix: Medium
Feature: UNDETERMINED	Function: UNDER REVIEW
Reported In Release: FI 07.3.00	Service Request ID: 1277602

Defect ID: DEFECT000491622	Technical Severity: High
Summary: In ICX64xx devices, 1G copper port goes down due to InErrors.	
Symptom: The "show interface" command shows the interface as being down even though the link LED is lit and the interface at the other end of the link is up.	
Probability: Low	
Feature: Platform	Function: 1G Link
Reported In Release: FI 07.4.00	Service Request ID: 1198350,1195320

Defect ID: DEFECT000491696	Technical Severity: High
Summary: Newly connected DHCP client does not get IP address, if it is connected after active unit power down without stack MAC configuration (new active programming bad entries into the trunk table due to this misconfiguration)	
Symptom: New DHCP client does not get IP address, if it is connected after active unit power down.	
Probability: High	
Feature: FI Infrastructure	Function: stacking configuration
Reported In Release: FI 07.4.00	Service Request ID: 1228098

Defect ID: DEFECT000494806	Technical Severity: High
Summary: Issuing a "show log" command causes the unit to reload unexpectedly.	
Symptom: Device reloads unexpectedly while cold rebooting the device with the below configurations logging buffered 100 logging persistence	
Probability: Medium	
Feature: Platform	Function: KERNEL
Reported In Release: FI 07.4.00	Service Request ID: 1292090,1291263

Defect ID: DEFECT000495058	Technical Severity: High
Summary: Keepalive LAG on new active flaps when standby unit (old active) joins the stack after stack failover	
Symptom: Keepalive LAG on new active flaps when standby unit (old active) joins the stack after stack failover	
Probability: High	Risk of Fix: Medium
Feature: FI Infrastructure	Function: stacking unknown
Reported In Release: FI 08.0.10	Service Request ID:

Defect ID: DEFECT000495059	Technical Severity: High
Summary: UDLD link on new active flaps when standby unit (old active) joins the stack after stack failover	
Symptom: UDLD link on new active flaps when standby unit (old active) joins the stack after stack failover	
Probability: High	Risk of Fix: Low
Feature: FI L2	Function: Control Plane - UDLD Protected Link Groups
Reported In Release: FI 08.0.10	Service Request ID: ...

Defect ID: DEFECT000496526	Technical Severity: Medium
Summary: Large flushes are seen in "show log" command output with logging persistence enabled.	
Symptom: Large flushes counter seen in "show log" command output after doing a cold reboot, clear log and show log.	
Probability: Medium	
Feature: FI Embedded Management	Function: SYSLOG
Reported In Release: FI 07.4.00	Service Request ID: 1294181

Defect ID: DEFECT000497211	Technical Severity: High
Summary: FastIron device (ICX6450 with DHCP enabled) hangs during DHCP client (Win7 PC) requests	
Symptom: When configuring ICX6450 (8.0.01b or 7.4.00e routing code) with two DHCP pools and assign them to two VLANs, if we move a PC running Windows 7 (DHCP client) between VLANs, the device will stall for some time. The console/serial does not response during this time; the CPU usage goes up to 99%.	
Probability: Medium	Risk of Fix: Low
Feature: FI Embedded Management	Function: DHCP IPv4 Client/Server
Reported In Release: FI 08.0.01	Service Request ID: 1287692

Defect ID: DEFECT000498541	Technical Severity: Medium
Summary: Configuring a new read only community name fails to update the default read-only community name "public"	
Symptom: Device will respond to SNMP get or walk with the default read-only community name "public" even after the new read only community name is configured.	
Probability: Medium	
Feature: FI Embedded Management	Function: SNMP v1/v2/v3
Reported In Release: FI 07.4.00	Service Request ID: 1300064

Defect ID: DEFECT000498678	Technical Severity: High
Summary: ARP entry is deleted when primary interface of LAG is deleted during failover	
Symptom: When pulling the power, or failing over via CLI from stack unit one to stack unit two of core / routing device, line protocol comes up on the corresponding link on the edge switch before core has full stabilized. Additionally, for a subset of hosts there are still connectivity problems when traffic needs to be routed to a different subnet.	
Probability: High	
Feature: Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.4.00	Service Request ID: 1300008

Defect ID: DEFECT000500413	Technical Severity: High
Summary: RSTP will flap periodically while sending multicast traffic	
Symptom: RSTP will flap periodically while sending multicast traffic in high rate	
Probability: High	
Feature: L2/L3 Multicast Features	Function: IGMP snooping and variants
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000504186	Technical Severity: Medium
Summary: In a stacked ICX6610, ARP request broadcasts are not sent from tagged ethernet ports of a virtual ethernet interface if there are untagged ethernet ports in the same VLAN which are down.	
Symptom: In an ICX6610 stack, could communicate with the hosts connected to untagged ethernet ports but unable to communicate with hosts connected via tagged ethernet ports. This is because that ICX sends ARP request broadcasts out only on untagged ethernet ports and not on tagged ethernet ports in the same VLAN which are down.	
Probability: Medium	
Feature: Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.4.00	Service Request ID: 1311621

Customer reported defects closed with code in Release 07.4.00e

Defect ID: DEFECT000391950	Technical Severity: Medium
Summary: The debug packet-capture filter format for destination and source MAC does not follow Brocade's standard for MAC address format and the CLI accepts Brocade's standard, but all MAC address octets are set to zero	
Symptom: No error was displayed on configuring filters using the non standard Brocade MAC address format for debug packet filters. This resulted in belief that the filter was applied when it was not really applied.	
Probability: Medium	
Feature: FI Embedded Management	Function: CLI Parser
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000396271	Technical Severity: High
Summary: For certain voice-vlan numbers, checksum for CDP packets fails.	
Symptom: This issue is seen with VoIP phones from certain vendors. With such devices there is loss of functionality upon reception of CDP packets.	
Probability: Low	Risk of Fix: Medium
Feature: FI Platform Specific features	Function: PoE/PoE+
Reported In Release: FI 07.3.00	Service Request ID: ,1179888

Defect ID: DEFECT000429167	Technical Severity: High
Summary: IP free reassembly list entries allocation failed error message displayed on console.	
Symptom: Re-assembly of IP packets fails in certain corner case scenarios where a larger IP packet is received.	
Probability: Low	
Feature: Layer 3 Forwarding - IPV4	Function: IP MTU & Fragmentation (IPV4)
Reported In Release: FI 07.4.00	Service Request ID: 1153427

Defect ID: DEFECT000441827	Technical Severity: High
Summary: A few IP security camera brands fail to power on when connected to ICX6610	
Symptom: IP security camera fails to power on when connected to ICX6610. The "show inline power" output on the ICX6610 displays the camera port in a "short circuit" state.	
Probability: High	Risk of Fix: Low
Feature: Power over Ethernet	Function: Power over Ethernet
Reported In Release: FI 07.3.00	Service Request ID: 1110403

Defect ID: DEFECT000448184	Technical Severity: High
Summary: ICX6610 stack unstable due to interface errors (e.g. CRC, "InErrors", "InGiantPkts", "InJabber" and/or "InBadPkts") on the stacking ports	
Symptom: CPU utilization steadily increases, interface errors are seen on some of the stacking links, and the unit generating the errors eventually breaks away from the stack.	
Workaround: The separated stack unit needs to be cold booted to recover.	
Probability: Low	Risk of Fix: Medium
Feature: FI Platform	Function: 40G Link
Reported In Release: FI 07.3.00	Service Request ID: 1148013,1149815

Defect ID: DEFECT000448876	Technical Severity: Medium
Summary: With DHCP snooping enabled, IP cache is not updated from "Drop" to "Forward" when ARP packet is received	
Symptom: Traffic loss to certain destinations is observed when traffic transits through a VRRP backup router if DHCP snooping is enabled on the incoming interface.	
Probability: Low	Risk of Fix: High
Feature: SX L2 Forwarding	Function: MAC Table/FDB Manager
Reported In Release: FI 07.2.00	Service Request ID: 1105581

Defect ID: DEFECT000458866	Technical Severity: Medium
Summary: The status of ICMP redirect is not displayed in the output of "show ip" or "show ip interface"	
Symptom: The output of "show ip (show ipv6)" and "show ip int" displays the status of ICMP redirect incorrectly.	
Probability: Medium	
Feature: Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.4.00	Service Request ID: 1170836

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

Defect ID: DEFECT000464240	Technical Severity: High
Summary: IP Helper Address stops working after the DHCP server feature is enabled and disabled	
Symptom: DHCP client broadcast requests are not forwarded to the IP Helper Address after enabling and disabling the DHCP server on the device.	
Workaround: Re-enable DHCP Server, even if not using the switch for that purpose.	
Probability: Medium	Risk of Fix: High
Feature: FCX L2 Forwarding	Function: DHCP assist
Reported In Release: FI 07.3.00	Service Request ID: 1179152

Defect ID: DEFECT000464627	Technical Severity: High
Summary: CPU Memory Leak may be observed when IP DHCP Server is enabled	
Symptom: If DHCP Server is configured on the FI device without a DHCP Scope, a slow CPU memory leak may be observed.	
Workaround: Ensure DHCP Scope on external DHCP Server is correctly configured.	
Probability: Low	Risk of Fix: Medium
Feature: FI Embedded Management	Function: DHCP
Reported In Release: FI 07.3.00	Service Request ID: 1179149

Defect ID: DEFECT000464973	Technical Severity: Medium
Summary: Issuing the "show media slot <num>" command causes sending and receiving of VRRP-E Hello packets to stop for more than three seconds, leading to VRRP-E status flaps.	
Symptom: VRRP-E master/backup flaps and Duplicate IP Address messages are seen when the "show media slot 1" command is executed on either ICX6650 in a VRRP-E hot standby pair.	
Probability: High	Risk of Fix: Low
Feature: Optics	Function: OPTICS
Reported In Release: FI 07.5.00	Service Request ID: 1186282

Defect ID: DEFECT000465151	Technical Severity: High
Summary: VLAN configuration via SNMPset is missing after stack switchover	
Symptom: Network configuration lost due to missing VLAN settings.	
Workaround: This appears to impact SNMPv3 only. If customer creates a SNMPv2c read-write community, this issue doesn't appear to take place - the VLAN changes are replicated properly to the other units in the running-configuration.	
Risk of Fix: Medium	
Feature: FI Embedded Management	Function: SNMP
Reported In Release: FI 08.0.00	Service Request ID: 1192392

Defect ID: DEFECT000467435	Technical Severity: Medium
Summary: Interface stays down intermittently after reload in ICX6450 and ICX 6430 SKUs	
Symptom: The "show interface" command shows the interface as Down even though the link LED is lit and the interface at the other end of the link is up..	
Workaround: Reloading will resolve the issue.	
Probability: Low	
Feature: Platform	Function: 1G Link
Reported In Release: FI 07.4.00	Service Request ID: 1198350,1195320

Defect ID: DEFECT000467796	Technical Severity: Medium
Summary: SX-FI-8XG line card improperly evaluates ACL for switched traffic within a VLAN	
Symptom: When an ACL is configured on a VE interface, it gets applied to switched traffic within the VLAN as well, whereas it is expected to be applied only on routed traffic.	
Probability: High	Risk of Fix: Medium
Feature: FI - L4/Security	Function: IPV4 ACLs - SX
Reported In Release: FI 07.3.00	Service Request ID: 1198247

Defect ID: DEFECT000467830	Technical Severity: Medium
Summary: Traffic through LAG is interrupted on standby unit when active unit is reloaded.	
Symptom: Problem is seen on a stack of two ICX6610 switches with a LAG group consisting of one port in the active unit and another port in the standby unit. When the active unit is reloaded, the egress traffic through LAG group on standby stops for about 30 seconds.	
Probability: Low	
Feature: L2 Forwarding	Function: UNDETERMINED
Reported In Release: FI 07.4.00	Service Request ID: 1199002

Defect ID: DEFECT000467837	Technical Severity: Medium
Summary: The source IPv6 address for the router advertisement should be the Link Local Address, not the VRRP Address.	
Symptom: The VRRP address is used as the Source IPv6 address in router advertisements, whereas only the Link Local Address should be used.	
Probability: High	Risk of Fix: Low
Feature: FI L3 Unicast	Function: Control Plane - VRRPv3 for IPv6
Reported In Release: FI 07.3.00	Service Request ID: 1191608

Defect ID: DEFECT000469631	Technical Severity: High
Summary: MAC Table flush in a fully populated chassis can cause STP flaps	
Symptom: When an 802.1d enabled port flaps, it leads to a flush of the MAC Table, creating a high CPU condition lasting for up to a minute which then causes other protocols to flap as well.	
Probability: Low	Risk of Fix: Medium
Feature: FCX L2 Control	Function: Spanning Tree Protocols
Reported In Release: FI 07.3.00	Service Request ID: 1157674

Defect ID: DEFECT000469670	Technical Severity: Medium
Summary: The ICX6610 incorrectly uses the interface MAC as the Source MAC address in VRRP-E Gratuitous ARP packets.	
Symptom: VRRP-E Gratuitous ARP packets are sent with Interface MAC as the source MAC address, whereas they should use the VRRP-E Virtual MAC address.	
Probability: High	
Feature: Layer3 Control Protocols	Function: VRRP/VRRP-E and slow-start timer-VRRP-E timer scale
Reported In Release: FI 07.4.00	Service Request ID: 1206999

Defect ID: DEFECT000471200	Technical Severity: High
Summary: ICX6610 reset due to Data TLB error in corner case scenarios upon receiving certain control plane stacking messages from the peer units.	
Symptom: ICX6610 reset due to Data TLB error in corner case scenarios upon receiving certain control plane stacking messages from the peer units.	
Probability: Low	
Feature: FI Infrastructure	Function: Stacking table sync/high availability
Reported In Release: FI 07.4.00	Service Request ID: 1212599

Defect ID: DEFECT000471789	Technical Severity: Critical
Summary: In rare cases, DHCP offer packets that are received on a VE interface cause the device to reload.	
Symptom: In rare cases, DHCP offer packets that are received on a VE interface overwrite the IPv6 default route entry causing the device to reload.	
Probability: Low	Risk of Fix: Low
Feature: FI Embedded Management	Function: DHCP
Reported In Release: FI 07.5.00	Service Request ID: 1213962

Defect ID: DEFECT000472419	Technical Severity: High
Summary: Jabber errors seen for SFP/SFP+ ports 1/2/1 to 1/2/4 while in 1000-full-master speed-duplex mode between two ICX6450 units	
Symptom: If you connect two ICX 6450 devices with the 1/2/1 and 1/2/4 stacking ports in 1Gbps, duplex speed, 1000-full-master mode, the uplink has jabber errors and is unable to forward data.	
Workaround: Currently, there is no workaround	
Probability: Medium	
Feature: Platform	Function: 1G Link
Reported In Release: FI 07.4.00	Service Request ID: 1215380

Defect ID: DEFECT000472837	Technical Severity: High
Summary: Adding an uplink switch causes duplication of multicast traffic.	
Symptom: Adding an uplink switch X/Y/Z in a VLAN causes duplication of multicast traffic.	
Probability: Medium	
Feature: FI L3 Multicast	Function: Forwarding - TI L3 Multicast
Reported In Release: FI 08.0.00	

Defect ID: DEFECT000473641	Technical Severity: High
Summary: On the TI-24X device, the port 1 flaps continuously when it is connected to another device.	
Symptom: On the TI-24X device running 07.4.00d software version, the port 1 flaps continuously when it is connected to another device.	
Probability: High	
Feature: Platform	Function: System
Reported In Release: FI 07.4.00	Service Request ID: 1213385,1234640

Defect ID: DEFECT000473852	Technical Severity: Medium
Summary: Protected link on a PLG group stops forwarding traffic on powering down the active unit	
Symptom: Protected links are configured on ports on both Active and Standby units. After active unit is powered off, the active protected link stops forwarding.	
Probability: Medium	
Feature: L2 Forwarding	Function: Protected Link group
Reported In Release: FI 07.4.00	Service Request ID: 1225731

Defect ID: DEFECT000474185	Technical Severity: High
Summary: Device acting as DHCP-Relay Agent can unexpectedly reload while updating its ARP table	
Symptom: In certain scenarios, the device acting as DHCP-Relay may reset while updating its ARP table from DHCP-ACK packet	
Probability: High	
Feature: UNDETERMINED	Function: UNDETERMINED
Reported In Release: FI 07.4.00	Service Request ID: 1226009

Defect ID: DEFECT000475396	Technical Severity: Medium
Summary: Combo ports on member units of a FCX stack takes longer time to forward traffic	
Symptom: Combo ports on member units of a FCX stack takes longer time to forward traffic	
Probability: Medium	
Feature: FI Infrastructure	Function: Stacking table sync/high availability
Reported In Release: FI 07.4.00	Service Request ID: 1231326

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

Defect ID: DEFECT000478555	Technical Severity: Medium
Summary: Removing the dual mode configuration on an interface configured with dot1x and mac authentication causes the switch to unexpectedly reload.	
Symptom: Removing “no dual-mode” on an interface configured with dot1x and mac authentication causes the switch to unexpectedly reload.	
Probability: High	
Feature: FI ACL	Function: 802.1x authentication
Reported In Release: FI 07.4.00	Service Request ID: 1179303

Defect ID: DEFECT000479288	Technical Severity: High
Summary: When network failure occurs with IGMPv3 and IGMP Tracking enabled, it causes delay in failover process.	
Symptom: When network failure occurs with IGMPv3 and IGMP Tracking enabled, it causes delay in failover process.	
Probability: High	
Feature: L2/L3 Multicast Features	Function: IGMP snooping and variants
Reported In Release: FI 07.4.00	Service Request ID: 1241536

Defect ID: DEFECT000481649	Technical Severity: High
Summary: Counter overflow causes an ICX 6650 device to stop functioning after 9999 reloads.	
Symptom: Counter overflow causes an ICX 6650 device to stop functioning after 9999 reloads.	
Probability: High	
Feature: Platform	Function: UNDETERMINED
Reported In Release: FI 07.4.00	Service Request ID: 1241878

Defect ID: DEFECT000483166	Technical Severity: Medium
Summary: ICX 6450-48P switches acoustics is high.	
Symptom: Noise from the fan is not at the desirable levels on ICX6450-48P devices.	
Probability: Medium	
Feature: Platform	Function: Chassis - EEPROM/flash/LED/Fan/TempSensor/PSU
Reported In Release: FI 07.4.00	

Customer reported defects closed with code in Release 07.4.00d1

Defect ID: DEFECT000473641	Technical Severity: High
Summary: Port 1 on TI-24x flaps continuously when connected to another device.	
Symptom: Port 1 on TI-24x running FI 07.4.00d code flaps continuously when connected to another device. Problem is not seen with other ports on the TurboIron device.	
Workaround: Use any other port on TurboIron other than port 1.	
Probability: High	Risk of Fix: Low
Feature: Platform	Function: System
Reported In Release: FI 07.4.00d	Service Request ID: 1213385,1234640

Customer reported defects closed with code in Release 07.4.00d

Defect ID: DEFECT000296833	Technical Severity: Medium
Summary: Device will close a Telnet management session when it receives a FIN even if output is pending.	
Symptom: Device will close a Telnet management session when it receives a FIN even if output is pending.	
Probability: High	Risk of Fix: Medium
Feature: FCX Management Functionality	Function: IPV4/V6 Telnet Service
Reported In Release: FI 07.0.01	Service Request ID: 246740

Defect ID: DEFECT000387658	Technical Severity: High
Summary: In ICX6450, when 1 Gbps copper SFP is inserted in a fiber port, the port may not be operational.	
Symptom: In ICX6450, when 1 Gbps copper SFP is inserted in a fiber port, the port may not be operational.	
Workaround: You can either toggle the port state from CLI or physically hot-swap the SFP.	
Probability: Low	
Feature: Platform	Function: 1G Link
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000391531	Technical Severity: Medium
Summary: In TurboIron, when a copper SFP is moved from port 1 to 2 and then back to 1, the link does not come up without reloading the device.	
Symptom: In TurboIron, when a copper SFP is moved from port 1 to 2 and then back to 1, the link does not come up without reloading the device.	
Workaround: You can bounce the port to fix the problem – unlike in 7.3.00c where you had to reload the device to recover.	
Probability: High	Risk of Fix: Low
Feature: Optics	Function: OPTICS
Reported In Release: FI 07.3.00	Service Request ID: 711623

Defect ID: DEFECT000392549	Technical Severity: Medium
Summary: VRRP-E flaps when you add or remove ports from a VLAN through Web Management interface.	
Symptom: VRRP-E flaps when you add or remove ports from a VLAN through Web Management interface.	
Workaround: You should add or delete ports from CLI.	
Probability: Medium	Risk of Fix: Low
Feature: FCX Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	Service Request ID: 693427,1198545

Defect ID: DEFECT000400311	Technical Severity: High
Summary: The "dot1x auth-timeout-action" command does not differentiate between success and failure configurations.	
Symptom: In failure configurations, the port moves to the native VLAN that is configured as part of the "dot1x auth-timeout-action success" configuration even when the "dot1x auth-timeout-action failure" command configures the port to move into the restricted VLAN.	
Probability: Medium	Risk of Fix: Low
Feature: FI - L4/Security	Function: 802.1x
Reported In Release: FI 07.5.00	Service Request ID: 1104525

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

Defect ID: DEFECT000406877	Technical Severity: Medium
Summary: ARP inspection fails to inspect ARP response packet.	
Symptom: ARP inspection fails to inspect ARP response packet.	
Probability: High	Risk of Fix: Medium
Feature: FI - L4/Security	Function: Dynamic ARP inspection
Reported In Release: FI 07.3.00	Service Request ID: 739235

Defect ID: DEFECT000408208	Technical Severity: High
Summary: Configuring monitor port unexpectedly reloads the active stack controller if a module has been changed in the FCX stack.	
Symptom: Both stack units 3 and 2 are powered off and FCX XFP 10G module is swapped from unit 3 to unit 2. Then, both unit 2 and unit 3 are powered up, and the stack was configured by entering "module 3 fcx-xfp-2-port-10g-module" command on stack unit 2 and "no module 3 fcx-xfp-2-port-10g-module" command on stack unit 3. A write memory (wr mem) command was then issued to save the configuration. Subsequently, commands "mirror-port ether 1/1/1", "int ether 3/1/22", and "monitor ether 1/1/1 both" are configured. This causes the active stack controller to perform an expected reset. And, the standby stack controller takes over as the active stack controller. Then configuring a monitor port on e 3/1/22 caused the new active to perform an unexpected reset. After these two resets, no more resets were observed.	
Workaround: Do not configure the stack with the "no module 3 fcx-xfp-2-port-10g-module" command even after the module is removed from the system. This will prevent the running configuration and static configuration getting out of sync, causing data structure access issue in module 3. This will not affect system operation.	
Probability: High	Risk of Fix: Low
Feature: FI Infrastructure	Function: port mirroring/monitoring
Reported In Release: FI 07.3.00	Service Request ID: 746263

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

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

Defect ID: DEFECT000410277	Technical Severity: High
Summary: Switch reloads when non-PoE port receives a CDP message.	
Symptom: After upgrade from 07.2.02e to 07.3.00c, the switch reloads continuously.	
Workaround: Disable CDP on FWS or all devices connected to FWS.	
Probability: High	Risk of Fix: Low
Feature: FI Platform	Function: POE
Reported In Release: FI 07.3.00	Service Request ID: 748591

Defect ID: DEFECT000415140	Technical Severity: Medium
Summary: DHCP server does not allocate addresses for all hosts within the defined address pools.	
Symptom: Some host DHCP requests fail, while other requests for hosts on the same VLAN are successful.	
Probability: High	
Feature: Platform	Function: System
Reported In Release: FI 07.4.00	Service Request ID: 1061154

Defect ID: DEFECT000415181	Technical Severity: Medium
Summary: Multicast packets are duplicated to 224.0.0.x across ICX6610 Layer 2.	
Symptom: Multicast packets are duplicated to 224.0.0.x across ICX6610 Layer 2.	
Probability: High	
Feature: L2 Forwarding	Function: Other
Reported In Release: FI 07.4.00	Service Request ID: 737715

Defect ID: DEFECT000419248	Technical Severity: Medium
Summary: Spanning tree blocked port forwards ARP broadcasts.	
Symptom: In SX device, enabling a redundant link in a VLAN may occasionally cause loop in the network.	
Probability: Medium	Risk of Fix: Low
Feature: SX L2 Control	Function: Spanning Tree Protocols
Reported In Release: FI 07.2.02	Service Request ID: 841043

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

Defect ID: DEFECT000422811	Technical Severity: Medium
Summary: Stack ID is swapped when Ring Stack is changed to Linear Stack due to port related issues.	
Symptom: Stack ID could be swapped when Ring stack is changed to Linear stack due to port related issues.	
Workaround: Make the units clean with "unconfigure clean" command and then allow the units to join the stack again.	
Probability: Medium	Risk of Fix: Medium
Feature: FI Infrastructure	Function: stacking undetermined
Reported In Release: FI 07.3.00	Service Request ID: 1091448

Defect ID: DEFECT000423085	Technical Severity: Medium
Summary: PoE on SX can get stuck due to power glitch. Device is not providing inline power and may show incorrect information.	
Symptom: SX device may stop providing power to PDs such as access points and IP phones. PoE module is showing incorrect inline power allocation, even when no PD is attached.	
Workaround: The fix is available from 07.2.02h, and is also available in 07.4.x.	
Probability: Medium	Risk of Fix: Low
Feature: POE FW upgrade	Function: POE FW upgrade
Reported In Release: FI 07.2.02	Service Request ID: 760185

Defect ID: DEFECT000425786	Technical Severity: Medium
Summary: IEEE PD class 0 default power allocation should be set to 15.4 Watts instead of 30 Watts.	
Symptom: Due to incorrect power allocation of IEEE PD class 0 by switch, the device suffers from power budget issue. To supply enough inline power for all the PDs in use, manual configuration is required on all switches to trim the power budget.	
Workaround: Use CLI command "inline power power-limit 15400" to configure power allocation.	
Probability: High	Risk of Fix: Low
Feature: Power over Ethernet	Function: Power over Ethernet
Reported In Release: FI 07.3.00	Service Request ID: 1090929

Defect ID: DEFECT000426653	Technical Severity: Medium
Summary: Switch performs unexpected system reload when a loopback interface is enabled in ICX 6610.	
Symptom: Switch performs unexpected system reload when a loopback interface is enabled in ICX 6610.	
Workaround: Remove static route pointing to VE interface.	
Probability: High	
Feature: Layer3 Control Protocols	Function: OSPFV2 - IPV4
Reported In Release: FI 07.4.00	Service Request ID: 1097908

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

Defect ID: DEFECT000431548	Technical Severity: High
Summary: ACL programming in hardware may become inconsistent with software if ACLs are removed and added to the running configuration through TFTP server.	
Symptom: After an ACL associated with PBR configuration is removed and added to the running configuration through TFTP server, the PBR functionality may no longer work as expected.	
Workaround: Do not add or remove ACLs to the running configuration through TFTP, and instead manually add ACLs through CLI.	
Probability: Medium	Risk of Fix: Medium
Feature: FI ACL	Function: ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.3.00	Service Request ID: 1051833

Defect ID: DEFECT000433752	Technical Severity: Medium
Summary: Transient L2 loop may exist when old Active Controller is powered OFF and then ON.	
Symptom: L2 loop is seen for about 10 seconds, when Active controller is powered OFF and then ON.	
Probability: Medium	
Feature: FI Infrastructure	Function: stack switchover
Reported In Release: FI 07.4.00	Service Request ID: 1101656

Defect ID: DEFECT000435109	Technical Severity: High
Summary: When an active 10G link is changed to 1G and then back to 10G, the link fails to come up on 10G.	
Symptom: 10G fiber link is down/down.	
Feature: Platform	Function: 10G Link
Reported In Release: FI 07.4.00	Service Request ID: 1110023

Defect ID: DEFECT000435779	Technical Severity: High
Summary: In global configuration mode, STP or RSTP priority may not be saved after a reload.	
Symptom: STP priority in global mode is not preserved after a reload and defaults back to 8000.	
Workaround: Configure the spanning tree priority in VLAN mode; vlan 1 name DEFAULT-VLAN by port spanning-tree priority 16000	
Probability: Medium	Risk of Fix: Low
Feature: SX L2 Control	Function: SpanningTree Protocols
Reported In Release: FI 07.3.00	Service Request ID: 1110353

Defect ID: DEFECT000437017	Technical Severity: Medium
Summary: MAC address entry for IEEE 802.1X (0180.c200.0003) is created for each VLAN in ICX/FCX platform despite dot1x feature not enabled.	
Symptom: Flooding of packets with unicast destination MAC address seen when lots of VLANs are created.	
Probability: Low	
Feature: FI L2 control	Function: Other
Reported In Release: FI 07.4.00	Service Request ID: 1127192

Defect ID: DEFECT000438420	Technical Severity: Medium
Summary: Interface level negotiation mode configuration may not work correctly.	
Symptom: If global level negotiation configuration is deleted, interface level negotiation configuration may not take effect.	
Workaround: Configure interface level negotiation mode again.	
Probability: Medium	Risk of Fix: Medium
Feature: FCX Layer1 features	Function: Auto Negotiation
Reported In Release: FI 07.2.02	Service Request ID: 1131822

Defect ID: DEFECT000439145	Technical Severity: Medium
Summary: If you move cards from one slot to another and then issue the 'no module <module type>' command for the old slot, the management module reloads.	
Symptom: If you move cards from one slot to another and then issue the 'no module <module type>' command for the old slot, the management module reloads.	
Feature: Platform	Function: Chassis - EEPROM/flash/LED/Fan/TempSensor/PSU
Reported In Release: FI 07.4.00	Service Request ID: 1129498

Defect ID: DEFECT000442378	Technical Severity: Medium
Summary: The "clock set" command runs with 4 minute difference on ICX 6430 device.	
Symptom: The "clock set" command runs with 4 minute difference on ICX 6430 device.	
Risk of Fix: Medium	
Feature: Platform	Function: Boot
Reported In Release: FI 08.0.00	Service Request ID: 1154268

Defect ID: DEFECT000443109	Technical Severity: Medium
Summary: Warning temperature is not configurable on FESX devices running versions 7.2.02 and later.	
Symptom: Warning temperature is not configurable on FESX devices running versions 7.2.02 and later.	
Risk of Fix: Low	
Feature: SX Platform Specific features	Function: Chassis/fan/powersupplies/temperature sensors
Reported In Release: FI 07.2.02	Service Request ID: 1137834

Defect ID: DEFECT000444065	Technical Severity: High
Summary: In rare cases, one of the stack links of a member unit may get administratively disabled even when the link is up, causing CPU to CPU communication between other units in the stack to become one-directional.	
Symptom: The "show stack connection" command output displays a warning about missing stacking link and many errors about one directional CPU to CPU messages, even when all stacking links are physically up.	
Probability: Low	
Feature: FI Infrastructure	Function: stacking port trunking
Reported In Release: FI 07.4.00	Service Request ID: 1148013

Defect ID: DEFECT000444230	Technical Severity: Medium
Summary: Stand Alone FCX with Stacking Disabled gets DOM errors on default Stack Ports (SFP+).	
Symptom: Stand Alone FCX with Stacking Disabled gets DOM errors on default Stack Ports (SFP+).	
Feature: Platform	Function: Digital Optical Monitoring
Reported In Release: FI 07.4.00	Service Request ID: 1144242

Defect ID: DEFECT000448990	Technical Severity: High
Summary: Qphy 2140 Revision is not supported during repeated enable / disable.	
Symptom: Qphy 2140 Revision is not supported during repeated enable / disable.	
Feature: Platform	Function: UNDETERMINED
Reported In Release: FI 07.4.00	Service Request ID: 1101644

Defect ID: DEFECT000449453	Technical Severity: High
Summary: Multi-session in-band SNMP bulk walk on the MAC table causes LACP timers to expire and leads to a link flap.	
Symptom: On ICX6610, two or more simultaneous in-band SNMP bulk walks on the MAC table may cause LACPDU's to not be sent out on time, thereby triggering a timeout and flap by the link partner.	
Probability: High	Risk of Fix: High
Feature: FI L2	Function: Control Plane - LACP
Reported In Release: FI 07.3.00	Service Request ID: 1131590

Defect ID: DEFECT000451227	Technical Severity: Medium
Summary: VRRP peer IP address is not pingable if we remove IP address from another physical interface.	
Symptom: If VRRP is configured between TurboIron and any adjacent device and if there is any physical interface with IP address, removing it will cause the TurboIron VRRP to lose connection to peer.	
Workaround: Reload the device.	
Probability: High	Risk of Fix: Medium
Feature: TI Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	Service Request ID: 1120393

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

Defect ID: DEFECT000451871	Technical Severity: High
Summary: Link fails to come up on TurboIron copper SFP (1Gbps) when remote end switch is reloaded.	
Symptom: Link is not established on the affected port.	
Workaround: When port connected to GBIC is down and signal is detected, reset the PHY on GBIC to recover the port.	
Risk of Fix: Medium	
Feature: UNDETERMINED	Function: UNDETERMINED
Reported In Release: FI 07.3.00	Service Request ID: 1135987

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

Defect ID: DEFECT000454619	Technical Severity: Medium
Summary: When loop-detection and dot1x authentication is enabled on an interface, loop is not detected.	
Symptom: When dot1x is enabled on the ports of a VLAN and a physical L2 loop exists, there is high CPU usage.	
Workaround: Configure "dot1x port-control force-authorized" where loop is formed.	
Probability: Low	Risk of Fix: Medium
Feature: FI - L4/Security	Function: 802.1x
Reported In Release: FI 07.3.00	Service Request ID: 1136072

Defect ID: DEFECT000455824	Technical Severity: Medium
Summary: For FESX6 devices, the "show optic" command output is not correctly displayed.	
Symptom: FESX devices return "N/A" for "show optic <port#>" output if this command is executed before executing "show media" command.	
Feature: Platform	Function: Digital Optical Monitoring
Reported In Release: FI 07.4.00	Service Request ID: 1167129

Defect ID: DEFECT000457368	Technical Severity: High
Summary: Incorrect initialization of the downstream interface table may cause multicast congestion drops in a chassis with mixed generation line cards.	
Symptom: In very rare cases, multicast congestion drops occur on a third generation module in a mixed SX chassis, and multicast/broadcast packets will stop being transmitted on the ports of this module.	
Probability: Low	Risk of Fix: Medium
Feature: SX L2/L3 Multicast Features	Function: PIM Sparse
Reported In Release: FI 07.3.00	Service Request ID: 1113516

Defect ID: DEFECT000457828	Technical Severity: Medium
Summary: In some cases, SX-1600 may not boot up when 48-port 1 Gig copper modules are present in the system.	
Symptom: If 48-port 1Gig copper modules are present, SX chassis does not complete the boot process. In this error condition, the following error messages are displayed on the console: "qdLoadDriver return Failed QuarterDeck initialization failed. qdMultiDevStart Failed for Dev 20, Port 0 ERROR[puma_phy_init]: init_6165_interfaces returned 1 sx_1g_puma_init() failed [Error] :: Hw-validation-failure : read/write failed on line-module 11, powering it off "	
Probability: Medium	
Feature: Platform	Function: System
Reported In Release: FI 07.4.00	Service Request ID: 1169079

Defect ID: DEFECT000459312	Technical Severity: Medium
Summary: ICX device allows to enable multiple mirror ports for vlan mirroring and port mirroring. This mirrors the traffic to wrong mirror port.	
Symptom: ICX device allows to enable multiple mirror ports for vlan mirroring and port mirroring. This mirrors the traffic to wrong mirror port.	
Risk of Fix: Low	
Feature: FI Traffic conditioning and Monitoring	Function: port mirroring/monitoring
Reported In Release: FI 07.3.00	Service Request ID: 1168721

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

Defect ID: DEFECT000465359	Technical Severity: High
Summary: Enabling IGMP Snooping on Switch image may stop ARP Request packets from being processed.	
Symptom: On an SX system running Switch image with only Gen3 line modules, enabling "ip multicast passive" may prevent ARP Request packets from reaching the CPU for processing. Hence, connectivity to hosts is lost. This does not happen on Router image or on systems which have at least one older generation line module.	
Probability: High	Risk of Fix: Medium
Feature: SX L2/L3 Multicast Features	Function: IGMP snooping and variants
Reported In Release: FI 07.3.00	Service Request ID: 1152821

Defect ID: DEFECT000466704	Technical Severity: Medium
Summary: There is no syslog event when temperature exceeds the warning level on ICX 6430-24 fanless model.	
Symptom: There is no syslog event when temperature exceeds the warning level on ICX 6430-24 fanless model.	
Probability: High	
Feature: Platform	Function: Chassis - EEPROM/flash/LED/Fan/TempSensor/PSU
Reported In Release: FI 07.4.00	Service Request ID: 1179888

Customer reported defects closed with code in Release 07.4.00c

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

Defect ID: 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	Risk of Fix: Medium
Feature: SX L2 Forwarding	Function: MAC Table/FDB Manager
Reported In Release: FI 07.3.00	Service Request ID: 695827

Defect ID: DEFECT000389858	Technical Severity: Medium
Summary: "No PoD license for port <>" syslog message is generated only for active unit and not for member units	
Symptom: "PoD: No license present for port <> " syslog message is generated only for active unit in a stack setup.	
Probability: Medium	
Feature: FI Embedded Management	Function: SYSLOG
Reported In Release: FI 07.4.00	Service Request ID: 1034380

Defect ID: DEFECT000397535	Technical Severity: High
Summary: Wrong Fabric-link reported between linecard and backplane as down	
Symptom: wrong fabric-link reported between linecard and backplane as down	
Workaround: Add '1' to any slot reported in the log to understand the real slot affected by the link-failure	
Probability: High	
Feature: FI Debug support	Function: Platform
Reported In Release: FI 07.4.00	Service Request ID: 721607

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	Risk of Fix: Low
Feature: FCX Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	Service Request ID: 720777

Defect ID: DEFECT000399851	Technical Severity: Critical
Summary: CLI may encounter unexpected system reset when VLANs - for a large number of ports are being managed using the Web Management Interface	
Symptom: CLI may encounter unexpected system reset when VLANs - for a large number of ports are managed using the Web Management Interface.	
Probability: Medium	Risk of Fix: Medium
Feature: SX Network Management	Function: Web Management
Reported In Release: FI 07.3.00	Service Request ID: ,754515

Defect ID: DEFECT000403640	Technical Severity: High
Summary: It takes 6.7 seconds to clear the MAC addresses in router code where as it takes 400 milliseconds to flush it in switch code.	
Risk of Fix: Low	
Feature: Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.5.00	Service Request ID: 756077

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

Defect ID: DEFECT000410285	Technical Severity: Medium
Summary: Faulty line module failing initialization in an SX800 makes the System unusable.	
Symptom: A faulty module can make the system unusable and results in loss of network services. The system will attempt to reinitialize the module 3 times before going into a continuous reset cycle. Error messages such as the following will be seen: P1 : 02 03 F1 : 02 03 Module 2 Init failed with status 1 Err: Enabling module 2 Failed [1]Retrying ..	
Probability: Medium	Risk of Fix: Low
Feature: FI Platform	Function: Chassis/Cards/PCI - SX/TI
Reported In Release: FI 07.3.00	Service Request ID: 742229

Defect ID: DEFECT000410566	Technical Severity: Medium
Summary: Show tech can cause UDLD to flap in same rare scenario with a highly loaded chassis	
Symptom: In an SX chassis with several line cards full equipped with SFPs, when running a show tech, the show media command run by the show tech can cause some protocols such as UDLD to flap.	
Probability: Low	Risk of Fix: Low
Feature: SX Management Functionality	Function: CLI and parser
Reported In Release: FI 07.2.02	Service Request ID: 689327

Defect ID: DEFECT000411919	Technical Severity: Medium
Summary: Port Security with secure mac-address for violation shutdown is not working in FI 7.4.00	
Symptom: When we configure port security partially global and interface based, with shutdown as violation and the default maximum of one MAC address on the port. Changing host i.e. when plugging another laptop, the interface turns up and it changes the mac address of the new one learned from the recently connected device.	
Probability: High	
Feature: L2 Forwarding	Function: Port Mac security
Reported In Release: FI 07.4.00	Service Request ID: 753509

Defect ID: DEFECT000411951	Technical Severity: Medium
Summary: STP toggles after performing a CLEAR MAC on one of the remote MCT cluster switches.	
Symptom: STP could toggle during clear mac	
Probability: Low	Risk of Fix: High
Feature: FI L2 control	Function: Spanning-tree protocols /PVST+/PVRST+
Reported In Release: FI 07.5.00	Service Request ID: 743579, 756077

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

Defect ID: DEFECT000415496	Technical Severity: Medium
Summary: Named ACL is not implemented for SNMP community view restriction	
Symptom: When trying to use an ACL for a restricted SNMP view, named ACL is not accepted by the CLI.	
Workaround: Use numbered ACL	
Feature: FI Embedded Management	Function: CLI Parser
Reported In Release: FI 07.4.00	Service Request ID: 761241

Defect ID: DEFECT000415746	Technical Severity: Critical
Summary: FIPS Fatal Cryptographic Module Failure. Reason: CKR_VENDOR_DEFINED-FIPS ERROR. Current Seed is same as previous one. Resetting. Error shown on encrypted syslog	
Symptom: FIPS Fatal Cryptographic Module Failure. Reason: CKR_VENDOR_DEFINED stack: 20C78C14 2034EB30 200054CC 208DFFD0 20000534 20663904 200A41D0 200A4490 206A3308 20607BD0 20607CC0 20584CDC 20609CA8 5010 15B58 1AAF4 Rebooting(0)..	
Probability: Medium	Risk of Fix: Medium
Feature: FI Embedded Management	Function: Common Criteria
Reported In Release: FI 07.3.00	Service Request ID: 760187, 1057470

Defect ID: DEFECT000417423	Technical Severity: Medium
Summary: SYSLOG logout message happens only once irrespective of USER/ PRIVILEGE EXEC mode	
Symptom: The logout message appears when logout from PRIVILEGED EXEC to USER EXEC mode, even though the remote access connection still remains.	
Security: SSH logout by admin from src IP x.x.x.x, src MAC yyyy.yyyy.yyyy	
Workaround: As a workaround you can remove the following command. aaa authentication enable default local	
Probability: High	
Feature: FI Embedded Management	Function: SYSLOG
Reported In Release: FI 07.4.00	Service Request ID: 1033521 / 1034163

Defect ID: DEFECT000417524	Technical Severity: Medium
Summary: The output of the command "show media" is not printing the serial number for the optics.	
Symptom: The output of the command "show media" is not printing the serial number for the optics.	
Workaround: Use "dm optic 0/1/3 eep"	
Feature: Platform	Function: OPTICS
Reported In Release: FI 07.4.00	Service Request ID: 780969

Defect ID: DEFECT000419156	Technical Severity: Medium
Summary: BgpPeerFsmEstablishedTransitions OID does not increment on BGP flap	
Symptom: BgpPeerFsmEstablishedTransitions OID does not increment on BGP flap.	
Feature: FI Embedded Management	Function: SNMP v1/v2/v3
Reported In Release: FI 07.4.00	Service Request ID: 1089658

Defect ID: DEFECT000419924	Technical Severity: Medium
Summary: IP Source Guard blocks traffic after port moved to a new VLAN.	
Symptom: Unable to ping host after moving client to a new port which has Source-Guard enabled and then the port is moved to a new VLAN.	
Workaround: Disable source-guard on the port before moving it to the new VLAN and then re-enable source-guard after it has been moved.	
Probability: Medium	
Feature: FI ACL	Function: DHCP Snooping functionality
Reported In Release: FI 07.4.00	Service Request ID: 1071537

Defect ID: DEFECT000424362	Technical Severity: Medium
Summary: Unit may reload unexpectedly after run NO AGE in a port security enabled port.	
Symptom: Unit may reload unexpectedly after run 'no age' command in a port security enabled port and plug/unplug a new PC/host.	
Feature: L2 Forwarding	Function: Port Mac security
Reported In Release: FI 07.4.00	Service Request ID: 1092570

Defect ID: DEFECT000425462	Technical Severity: Medium
Summary: The previous fix DEFECT000419899 in 7.4.00b was only applied to FCX-F model. This new fix is applied to all FCX models.	
Symptom: Erroneous Syslog messages that report functioning FCX power supply units going down and coming up immediately are generated due to signal noise level. The symptom is the same with DEFECT000419899.	
Feature: Platform	Function: Chassis - EEPROM/flash/LED/Fan/TempSensor/PSU
Reported In Release: FI 07.4.00	Service Request ID: 723535

Defect ID: DEFECT000425958	Technical Severity: Medium
Summary: Switch encounters unexpected system reset after executing 'ip dhcp snooping vlan x' command	
Symptom: Switch may encounter unexpected system reset after executing 'ip dhcp snooping vlan' command in SX.	
Probability: High	
Feature: FI ACL	Function: DHCP Snooping functionality
Reported In Release: FI 07.4.00	Service Request ID: 1060660, 1042423

Defect ID: DEFECT000426410	Technical Severity: Medium
Summary: Device can reload unexpectedly after remove a port from an isolated PVLAN	
Symptom: Device may reload unexpectedly after a port is removed from an isolated PVLAN	
Probability: High	
Feature: L2 Forwarding	Function: Private VLAN
Reported In Release: FI 07.4.00	Service Request ID: 1100092

Defect ID: DEFECT000427550	Technical Severity: Medium
Summary: VRRP Standby may encounter port flap with multiple VLANs and VRIDs configuration.	
Symptom: Intermittent flaps on the VRRP standby may occur for multiple VRIDs in multiple VLANs configuration. Flap occurs only on the VRRP Standby and not on the VRRP Owner.	
Probability: Medium	Risk of Fix: 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: 1101971

Defect ID: DEFECT000428520	Technical Severity: Medium
Summary: Packet loss on SX module SX-FI-24GPP occurred due to multicast congestion	
Symptom: Packet loss may occur on SX-FI-24GPP modules due to multicast packet congestion	
Probability: Low	
Feature: Platform	Function: System
Reported In Release: FI 07.4.00	Service Request ID: 737265

Defect ID: DEFECT000429049	Technical Severity: Medium
Summary: High CPU observed with NETBIOS & DHCP broadcasts	
Symptom: High CPU observed in presence of DHCP & NETBIOS broadcasts.	
Probability: High	
Feature: Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.4.00	Service Request ID: 1092737

Defect ID: DEFECT000430373	Technical Severity: Critical
Summary: Unexpected System Reset on configuring/unconfiguring PMS	
Symptom: Unexpected System Reset on configuring/unconfiguring PMS .	
Risk of Fix: Low	
Feature: FI L2	Function: Forwarding - Port Mac Security
Reported In Release: FI 08.0.00	Service Request ID: 1119122

Defect ID: DEFECT000431290	Technical Severity: Medium
Summary: Issuing the “show dot1x mac-sessions ip-addr” command does not show the IP address even if the user is authenticated. The IP address field show N/A	
Symptom: “show dot1x mac-sessions ip-addr” do not show ip address even if user is authenticated. IP address field show N/A. Because of this, one of their applications do not work.	
Probability: High	
Feature: UNDETERMINED	Function: UNDETERMINED
Reported In Release: FI 07.4.00	Service Request ID: 1080868

Defect ID: DEFECT000431403	Technical Severity: Medium
Summary: IPv6 cache MAC address might not be updated after an IP movement in a HA scenario	
Symptom: Customer is moving an IPv6 VIP IP from one server to another and after the movement the IP is not reachable anymore.	
Workaround: clear ipv6 cache/neighbors	
Probability: Medium	
Feature: Layer 3 Forwarding - IPV6	Function: Data Forwarding (IPV6)
Reported In Release: FI 07.4.00	Service Request ID: 1100378

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

Defect ID: DEFECT000433237	Technical Severity: High
Summary: SNMP ifOperStatus reports ports in Blocking state as down even though the ports are physically and administratively up	
Symptom: FWS is incorrectly reporting the ifOperStatus as down(2), when the port is in blocking state but is administratively and operationally up.	
Probability: Medium	
Feature: FI Embedded Management	Function: SNMP v1/v2/v3
Reported In Release: FI 07.4.00	Service Request ID: 1115243

Defect ID: DEFECT000435603	Technical Severity: Medium
Summary: Secure MAC addresses get aged out in spite of constant flow of traffic when aging value is configured	
Symptom: When Port Security is configured with aging enabled, even though continuous traffic is sent, the Secure MAC address is still aged out and there is at least one packet lost at each age interval.	
Probability: High	
Feature: L2 Forwarding	Function: Port Mac security
Reported In Release: FI 07.4.00	Service Request ID: 1053635

Defect ID: DEFECT000436362	Technical Severity: Medium
Summary: The command "no snmp-server community public ro" cannot be saved in the startup-configuration and is therefore not retained after a reload	
Symptom: On the FWS648 immediately after the command "no snmp-server community public ro" is entered, the output of "show snmp sever" lists no communities, and the switch does not respond to SNMPv1. However, the command is not displayed in either the running configuration or the start-up configuration when a "write memory" is issued. After a switch reload, the SNMPv1 public community is reactivated.	
Probability: Medium	
Feature: FI Embedded Management	Function: SNMP v1/v2/v3
Reported In Release: FI 07.4.00	Service Request ID: 1115663

Defect ID: DEFECT000439112	Technical Severity: High
Summary: 30 Watts of power is allocated to PoE ports that are not even enabled during system boot up	
Symptom: Upon reloading the system under some circumstances, disabled ports are still allocated 30 Watts of power, potentially starving other ports that need it.	
Probability: High	
Feature: Platform	Function: Chassis - EEPROM/flash/LED/Fan/TempSensor/PSU
Reported In Release: FI 07.4.00	Service Request ID: 1128120

Customer reported defects closed with code in Release 07.4.00b

Defect ID: DEFECT000380727	Technical Severity: High
Summary: System Diagnostic feature is not functioning on TI products.	
Symptom: The "dm diag" CLI 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: DEFECT000400771	Technical Severity: Medium
Summary: FWS: If the usage of TCAM entries reaches near the maximum, a route entry could be overwritten by another route entry.	
Symptom: Routed traffic may not be forwarded to directly connected hosts in rare instances if the TCAM usage reaches near its maximum limit.	
Workaround: Clear the ARP cache and MAC table, then disable and re-enable the relevant IP interface.	
Probability: Low	Risk of Fix: Low
Feature: FCX Layer 3 Forwarding - IPV4	Function: Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	Service Request ID: 728137

Defect ID: DEFECT000409757	Technical Severity: Critical
Summary: System might reset when clearing dot1x mac-sessions with AAA accounting configured.	
Symptom: Switch might reset after on clearing dot1x authentication with AAA accounting enabled.	
Workaround: Do not enable AAA accounting, and do not clear dot1x mac-session.	
Probability: High	
Feature: FI ACL	Function: 802.1x authentication
Reported In Release: FI 07.4.00	Service Request ID: 742873

Defect ID: DEFECT000414044	Technical Severity: Medium
Summary: SNMP polling with Null username triggers a reject alert that can lead to a system reset	
Symptom: If an SNMP Client IP address list is configured and an SNMP request is received from a client that is not in this address list, a reject alert is correctly triggered but it causes the system to reset.	
Workaround: 1. Remove the SNMP Client list from the configuration in order to bypass the source IP address check for each SNMP request. 2. Configure an ACL to permit SNMP requests only from recognized clients.	
Probability: Medium	
Feature: FI Embedded Management	Function: SNMP v1/v2/v3 Traps
Reported In Release: FI 07.4.00	Service Request ID: 758521, 767795

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

Customer reported defects closed with code in Release 07.4.00a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of July 23, 2012.

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

Defect ID: 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: 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	Risk of Fix: Medium
Feature: FCX Management Functionality	Function: HTTPs/HTTP
Reported In Release: FI 07.2.02	Service Request ID: 697877

Defect ID: DEFECT000388641	Technical Severity: High
Summary: ICX 6430/50: Takes 3-4 minutes to release POE allocated power if there are no PDs connected or when ports go into overload state	
Symptom: When ports in the lower regions (1-30) are configured for PoE and not connected to any PoE devices, it may take up to 12 minutes for powering up PDs connected to a higher port region (31-48).	
Probability: Low	
Feature: Platform	Function: Chassis - EEPROM/flash/LED/Fan/TempSensor/PSU
Reported In Release: FI 07.4.00	

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	Risk of Fix: Medium
Feature: FCX Management Functionality	Function: HTTPs/HTTP
Reported In Release: FI 07.3.00	Service Request ID: 712561

Defect ID: DEFECT000390856	Technical Severity: High
Summary: ICX6430 Box could reset while displaying 'sh notification mac-movement threshold-rate'	
Symptom: ICX6430 Box could reset while displaying 'sh notification mac-movement threshold-rate'.	
Probability: Medium	
Feature: FI Embedded Management	Function: SNMP v1/v2/v3 Traps
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000390886	Technical Severity: Critical
Summary: Active unit might reset in a 3 unit stack when 5 or more SSH sessions are initiated to the stack.	
Symptom: System might reset when 5 or more SSH sessions are initiated to the ICX6450 3-unit stack.	
Probability: Low	
Feature: FI ACL	Function: ACL(all aspects of ACLs - IPv6)
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000391159	Technical Severity: High
Summary: When Hitless-reload is performed on secondary, MCT clients can get stuck in Down state, both for Local & Remote stat	
Symptom: In Dual MCT set up, when "Hitless-reload sec" command is executed on one of the MCT box, the LACP trunk stays down and the MCT client remains in Local/remote state.	
Probability: Medium	
Feature: FI MCT-L2	Function: Hitless
Reported In Release: FI 07.4.00	

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	Risk of Fix: Low
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: In ICX66xx, 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	Risk of Fix: Low
Feature: FI Infrastructure	Function: Flow Control
Reported In Release: FI 07.3.00	Service Request ID: 724451

Defect ID: DEFECT000395157	Technical Severity: High
Summary: ICX6450 port 1/2/2 and 1/2/4 configured for 1G requires reload to come up	
Symptom: ICX6450 port 1/2/2 and 1/2/4 configured for 1G do not come up and stays in the ERR-DISABLE state.	
Workaround: Reload the switch to bring up port 1/2/2 and 1/2/4 when configured for 1G	
Probability: High	
Feature: FI Embedded Management	Function: FPoD
Reported In Release: FI 07.4.00	Service Request ID: 721353

Defect ID: DEFECT000395775	Technical Severity: High
Summary: Ping to virtual IP fails after stack switchover, with IPv4 and IPv6 VRRP-E configured	
Symptom: IPv6 traffic from end hosts to VRRP-E cluster will get black holed. VRRP-E core functionality would stop working.	
Risk of Fix: Low	
Feature: FI L3 Unicast	Function: Control Plane - VRRPv2/VRRPE/VE Manager
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000396545	Technical Severity: Medium
Summary: Aggregate VLAN 802.1ad supports frame size only up to 1522 bytes instead of 1530 bytes	
Symptom: With 802.1ad configured, frame sizes only up to 1522 bytes are supported, instead of the expected 1530 bytes. Frames larger than 1522 bytes are dropped.	
Workaround: Configure jumbo frame support	
Probability: High	Risk of Fix: Low
Feature: FCX L2 Forwarding	Function: Q-in-Q
Reported In Release: FI 07.2.02	Service Request ID: 715413

Defect ID: DEFECT000397535	Technical Severity: High
Summary: Fabric link failure messages report the wrong value for the slot	
Symptom: Wrong fabric-link reported between linecard and backplane as down	
Workaround: Add '1' to any slot reported in the log to understand the real slot affected by the link-failure	
Probability: High	
Feature: FI Debug support	Function: Platform
Reported In Release: FI 07.4.00	Service Request ID: 721607

Defect ID: DEFECT000397736	Technical Severity: High
Summary: IPv6 ACL entry not getting programmed in TCAM after reload	
Symptom: ACL entry permitting the flow will not work and traffic will get implicitly denied.	
Workaround: Apply the IPv6 ACL after the stack is formed instead of storing it in the startup-config.	
Risk of Fix: Low	
Feature: FI ACL	Function: ACL(all aspects of ACLs - IPv6)
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000398319	Technical Severity: Medium
Summary: FCX rebooting continuously when GVRP is enabled	
Symptom: FCX reset continuously when GVRP is enabled and a VE interface is configured on the VLAN.	
Probability: High	
Feature: FI L2 control	Function: GVRP
Reported In Release: FI 07.4.00	Service Request ID: 724091,724091

Defect ID: DEFECT000398642	Technical Severity: Medium
Summary: Switch may reset when printing debug messages to all destinations under certain conditions	
Symptom: When using "debug destination all" in order to send the debug output to all the connected sessions, if Telnet password was previously enabled, the switch may experience a reset.	
Probability: High	
Feature: FI Embedded Management	Function: CLI Parser
Reported In Release: FI 07.4.00	Service Request ID: 724131

Defect ID: DEFECT000399554	Technical Severity: High
Summary: 10G license installation on ICX6450 box requires a reload for 10G ports to come up.	
Symptom: 10G ports are not coming UP after loading the 10G license. Need a reboot to make the ports work.	
Feature: FI Embedded Management	Function: Sw licensing
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000400064	Technical Severity: Medium
Summary: ARP packets embedded within 802.1ad is not forwarded by ICX6610 and ICX6450	
Symptom: ARP packets embedded within 802.1ad packet is not forwarded by ICX6610 and ICX6450	
Probability: High	Risk of Fix: Low
Feature: FCX L2 Forwarding	Function: Q-in-Q
Reported In Release: FI 07.3.00	Service Request ID: 728101, 716155

Defect ID: DEFECT000404254	Technical Severity: Critical
Summary: PVLAN - MAC learning not happening on community VLANs on reload of the box.	
Symptom: MAC learning is not happening on community VLANs even after a reload of the box.	
Workaround: Clear the MAC address every time, after a reload	
Feature: L2 Forwarding	Function: Private VLAN
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000406268	Technical Severity: Critical
Summary: ICX6430 system might reset on clicking the Web interface after stack-switch-over	
Symptom: ICX6430 system might reset on clicking the Web interface after stack-switch-over	
Feature: FI Embedded Management	Function: Web Management
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000406789	Technical Severity: Medium
Summary: Configuring and then removing Protocol VLAN does not clean up MAC Address Locking on port registers	
Symptom: High CPU due to data packets not being forwarded in hardware.	
Workaround: Perform "dot1x-enable" and then do "no dot1x-enable"	
Feature: L2 Forwarding	Function: Protocol VLAN
Reported In Release: FI 07.4.00	Service Request ID: 725439

Defect ID: DEFECT000407392	Technical Severity: Critical
Summary: System might reset while reloading or switchover when closing the SSH connection	
Symptom: System might reset while reloading or switching from Active to Standby, when closing the SSH connection.	
Feature: FI Embedded Management	Function: SSH/SCP
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000407946	Technical Severity: High
Summary: 1G to 10G speed change in ICX6450 brings up the remote port, even if the local port is in ERR-DISABLED (Reload the switch or stack to enable this port in 10G speed)	
Symptom: 1G to 10G speed change on an ICX6450 box makes the remote 10G port to come up which is not expected, even when the local 10G port remains in ERR-DISABLED state.	
Feature: Platform	Function: 10G Link
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000408948	Technical Severity: High
Summary: Incorrect spanning tree port state in hardware. Port should be in blocking but it is in forwarding.	
Symptom: High CPU is observed because of the possible L2 loop.	
Workaround: Disable the port on FCX before adding it to VLAN and then enable it.	
Probability: High	
Feature: FI L2 control	Function: Spanning-tree protocols /PVST+/PVRST+
Reported In Release: FI 07.4.00	Service Request ID: 747573

Defect ID: DEFECT000409496	Technical Severity: Critical
Summary: New active and member unit console could hang if previous active unit resets while doing supportsave	
Symptom: New active and member unit console could hang if previous active unit resets while collecting supportsave information.	
Feature: Platform	Function: supportsave
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000409721	Technical Severity: Medium
Summary: SNMP polling not functioning fully on ICX6430-24P	
Symptom: SNMP polling not functioning fully on ICX6430-24P because the device does not return the sysOID value correctly.	
Probability: High	
Feature: FI Embedded Management	Function: SNMP v1/v2/v3
Reported In Release: FI 07.4.00	Service Request ID: 749651

Customer reported defects closed with code in Release 07.4.00

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of March 5, 2012.

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

Defect ID: 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 yyyyyyyyyy. After a failover, the new Active will have this same LID and thus cannot be upgraded.	
Risk of Fix: Low	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.	
Risk of Fix: Low	Probability: Low
Feature: SX Layer1 features	Function: port flap dampening
Reported In Release: FI 07.2.00	Service Request ID: 624889

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. See example: router(config)#vlan-g 10 vlan 100 to 101 router(config-vlan-group-10)#tag e 24 Added tagged port(s) ethe 24 to vlan-group 10. router(config-vlan-group-10)#sh vlan 101 Error - port-vlan 101 does not exist. router(config-vlan-group-10)#	
Workaround: Create first VLAN using vlan-group then use "add-vlan" to add additional VLANs.	
Risk of Fix: Low	Probability: Medium
Feature: TI L2 Protocol	Function: VLAN GROUP
Reported In Release: FI TI 04.2.00	Service Request ID: 267889

Defect ID: DEFECT000345246	Technical Severity: Medium
Summary: When the FCX stack Master died (failover), the OSPF takes too long to converge for ECMP	
Symptom: After a failover, OSPF takes almost long time to converge and start forwarding traffic	
Risk of Fix: High	Probability: Low
Feature: FCX Layer3 Control Protocols	Function: OSPFV2 - IPV4
Reported In Release: FI 07.2.02	Service Request ID: 564661

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. System responds: Error in packet. Reason: undoFailed	
Workaround: Set the POE via the CLI	
Risk of Fix: Low	
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.	
Risk of Fix: Medium	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: 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.	
Risk of Fix: Low	
Feature: FCX Platform Specific features	Function: system bringup
Reported In Release: FI 07.2.02	Service Request ID: 643927

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.	
Risk of Fix: Low	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.	
Risk of Fix: Medium	Probability: High
Feature: FCX L2 Forwarding	Function: Private VLAN
Reported In Release: FI 07.2.02	Service Request ID: 650833,660501

Defect ID: DEFECT000364939	Technical Severity: Medium
Summary: FCX switch not honoring option 57	
Symptom: FCX sends 600 byte dhcp offer packet even with option 57 enabled	
Workaround: do not use option 57	
Risk of Fix: Low	Probability: Low
Feature: FCX DHCP	Function: Server
Reported In Release: FI 07.2.02	Service Request ID: 659331

Defect ID: DEFECT000365688	Technical Severity: High
Summary: [ICX][Regression] If copper GBIC is used in 10G port, After reload it does not come up. 1 out of 2 reloads.	
Symptom: [ICX] If copper GBIC is used in 10G port, After reload it does not come up. 1 out of 2 reloads.	
Risk of Fix: Low	Probability: Medium
Feature: FI Platform Specific features	Function: 10G Link
Reported In Release: FI 07.3.00	

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.	
Risk of Fix: Low	Probability: Low
Feature: SX_SYSTEM	Function: UNDETERMINED
Reported In Release: FI 07.2.02	

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.	
Risk of Fix: Low	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: 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	
Risk of Fix: Medium	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: DEFECT000371700	Technical Severity: Medium
Summary: When IP Helper is configured at runtime, RARP broadcast packets are not flooded in the VLAN	
Symptom: When IP Helper is configured at run-time, RARP broadcast packets are not flooded in the VLAN, although ARP broadcast packets are.	
Risk of Fix: Medium	Probability: High
Feature: SX L2 Forwarding	Function: DHCP assist
Reported In Release: FI 05.1.00	Service Request ID: 672885

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.	
Risk of Fix: Low	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	
Symptom: IP forwarding between FCX stack units may fail after switchover with mstp	
Workaround: Reload the whole stack again	
Risk of Fix: Medium	Probability: Medium
Feature: FCX L2 Control	Function: SpanningTree Protocols
Reported In Release: FI 07.3.00	Service Request ID: 681225

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.	
Risk of Fix: Medium	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	
Risk of Fix: High	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.	
Risk of Fix: Low	Probability: High
Feature: FI Infrastructure	Function: SX Hitless OS upgrade
Reported In Release: FI 07.3.00	Service Request ID: 680843

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

Defect ID: DEFECT000377048	Technical Severity: Medium
Summary: After stack failover causes preferred RIPv2 route to get deleted, backup Static route does not take over	
Symptom: If only the Active unit has RIP reachability and learns a better route than a configured Static route for a given IP Next Hop, upon disabling power to the Active unit, the ensuing failover does not move up the Static route as the best route on the new Active unit.	
Risk of Fix: Low	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.	
Risk of Fix: Low	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: 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.	
Risk of Fix: Low	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'.	
Risk of Fix: Low	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	
Risk of Fix: Medium	Probability: High
Feature: FCX Stacking	Function: stack-ports
Reported In Release: FI 07.2.02	Service Request ID: 686589

Defect ID: DEFECT000377544	Technical Severity: Medium
Summary: Started forwarding a packet even when the partner SYNC state is OFF in the LACP PDU.	
Symptom: A packet loss has been seen for up to 2 seconds on LACP link when old Stack Active unit powered up.	
Risk of Fix: Medium	
Feature: SX L2 Control	Function: LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.02	Service Request ID: 677389

Defect ID: DEFECT000377562	Technical Severity: Medium
Summary: Q-in-Q removes the original customer's tag for broadcast	
Symptom: After upgrading the code to 7300, broadcast packet is not forwarded at all in Q-in-Q environment.	
Risk of Fix: Medium	Probability: Medium
Feature: FCX L2 Forwarding	Function: Q-in-Q
Reported In Release: FI 07.3.00	Service Request ID: 682505

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".	
Risk of Fix: Low	Probability: High
Feature: SX Platform Specific features	Function: Management module redundancy
Reported In Release: FI 07.2.00	Service Request ID: 682807

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

Defect ID: DEFECT000378514	Technical Severity: Medium
Summary: One ICMP packet is lost every 60 seconds over a cross unit trunk when one switch in a stack of 2 goes down	
Symptom: In a stack of two FCX switches containing a 2-port trunk with one port on each chassis, if one of the switches is powered off, ICMP through the FCX shows one packet is lost every 60 seconds.	
Risk of Fix: Low	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: 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#>	
Risk of Fix: Low	Probability: High
Feature: Power over Ethernet	Function: Power over Ethernet
Reported In Release: FI 07.3.00	Service Request ID: 680137

Defect ID: DEFECT000379683	Technical Severity: Medium
Summary: [Pre-Existing] Cannot manage vlans via the web interface when there are a large number of ports	
Symptom: When add / remove ports from VLAN which has large number of ports via web interface, we might get this error message - "The "POST" request is too large for the internal work buffer:"	
Workaround: Use CLI	
Risk of Fix: Medium	Probability: Low
Feature: SX Management Functionality	Function: HTTPs/HTTP
Reported In Release: FI 07.2.00	Service Request ID: 690135

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

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".	
Risk of Fix: Medium	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 breaks if FCX stack reloaded and if only stdby comes UP	
Symptom: LACP breaks if FCX stack reloaded and if only stdby comes UP	
Risk of Fix: Medium	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.	
Risk of Fix: Low	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.	
Risk of Fix: Low	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 in Blocking if both stp and 802.1w configured after stack reload	
Symptom: FCX ports go in Blocking if both stp and 802.1w configured after stack reload	
Workaround: reload the whole fex stack again	
Risk of Fix: Medium	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.	
Risk of Fix: Low	Probability: Low
Feature: FCX L2 Forwarding	Function: Protected Link group
Reported In Release: FI 07.2.02	Service Request ID: 694309

Defect ID: DEFECT000383469	Technical Severity: Medium
Summary: A Layer 2 loop may be created if the Native VLAN Id is changed on other vendors' switches	
Symptom: If the Native VLAN Id is changed from the default on other vendors' switches that are connected to a Brocade device, a Layer 2 loop may result due to the Brocade device expecting an IEEE BPDU in the default VLAN 1.	
Workaround: Configure the Native VLAN to default value 1 on the other vendor's switch or configure VLAN 1 on the interface connected to the Brocade device.	
Risk of Fix: Low	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: Power supply front LEDs not working correctly.	
Risk of Fix: Low	
Feature: FI Platform	Function: Power Supply/Temp Sensor/Fan Controller
Reported In Release: FI 07.3.00	Service Request ID: 696305

Defect ID: DEFECT000385924	Technical Severity: Medium
Summary: IPv6 ve VRRPE ping to virtual IP timeouts after master->backup state change	
Symptom: Ping to virtual IPv6 VRRP-e not working after a failover.	
Workaround: Clear ipv6 cache and failover again.	
Risk of Fix: Low	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.	
Risk of Fix: Low	Probability: Low
Feature: FCX Stacking	Function: IPC Infrastructure
Reported In Release: FI 07.2.02	Service Request ID: 705189

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

Defect ID: DEFECT000387044	Technical Severity: High
Summary: FCX E/I shows PSU 2 as normal when inserted without power	
Symptom: 2nd PSU without power shows as normal and plugged in. Occurs in 7.202a, 7202f, and 7.3.	
Risk of Fix: Low	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.	
Risk of Fix: Low	Probability: High
Feature: FCX L2 Control	Function: LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.02	Service Request ID: 705571

Customer reported defects closed without code in Release 07.4.00

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of March 5, 2012.

Defect ID: DEFECT000315704	Technical Severity: High
Summary: VE interface's line protocol remains up even if interface itself is not	
Reason Code: Already Fixed in Release	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	Function: Virtual interface (ve) Manager
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000371093	Technical Severity: High
Summary: sFlow may not work on member units of an FGS stack	
Symptom: FGS and FLS are not supported in FI 7.4.00 release	
Workaround: Set the 'sflow polling-interval' to zero in order to send the sFlow samples.	
Reason Code: Not Applicable	Probability: High
Feature: FCX Network Management	Function: sFlow
Reported In Release: FI 07.2.02	

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.	
Reason Code: Not Applicable	Probability: Low
Feature: FCX Layer1 features	Function: Auto Negotiation
Reported In Release: FI 07.2.02	Service Request ID: 544899

Defect ID: DEFECT000361466	Technical Severity: Medium
Summary: Cannot communicate between Primary and Isolated Private VLANs	
Symptom: FGS and FLS are not supported in FI 7.4.00 release	
Reason Code: Not Applicable	Probability: High
Feature: SX L2 Forwarding	Function: Private VLAN
Reported In Release: FI 07.2.02	Service Request ID: 636621, 650833

Open defects

Open defects in Release 07.4.00a

This section lists defects with High or Medium Technical Severity as of July 23, 2012. Note that when a workaround to an issue is available, it is provided; otherwise, no recommended workaround is available at this time.

Defect ID: DEFECT000409757	Technical Severity: Critical
Summary: System might reset when clearing dot1x mac-sessions configured with AAA accounting.	
Symptom: Switch might reset after clearing 802.1x authentications with AAA accounting enabled.	
Workaround: Do not enable AAA accounting, or do not clear dot1x mac-session	
Feature: FI ACL	Function: 802.1x authentication
Service Request ID: 742873	
Reported In Release: FI 07.4.00	Probability: High

Defect ID: DEFECT000401640	Technical Severity: High
Summary: LLDP on 10G port on ICX6450 does not work after the "stack port" is configured as the "Data port"	
Symptom: LLDP on 10G port on ICX6450 does not work after the "stack port" is configured as the "Data port"	
Feature: FI Embedded Management	Function: LLDP
Reported In Release: FI 07.4.00	Probability: High

Defect ID: DEFECT000404478	Technical Severity: High
Summary: ICMPv6 messages that are higher than the outgoing port default MTU (1500) are not sent by the device to host.	
Symptom: Path MTU discovery on FCX/ICX6610 does not work correctly when outbound MTU on interface is configured to 1500.	
Workaround: This issue is seen only if interface MTU is configured as 1500 and jumbo is enabled. For any other MTU configurations the issue will not be there.	
Feature: Layer 3 Forwarding - IPV6	Function: Path MTU discovery for IPV6 (RFC 1981)
Reported In Release: FI 07.4.00	Probability: Medium

Defect ID: DEFECT000406745	Technical Severity: High
Summary: After reload of an MCT node, client ports go into STP forwarding state if SSTP is configured in the node.	
Symptom: MCT client ports are going into STP forwarding state (single span configured) when MCT node comes up after reload. Due to this MCT clients would start receiving STP BPDUs from MCT nodes.	
Workaround: Disable/enable SSTP (single span) on MCT nodes	
Feature: FI MCT-L2	Function: Spanning Tree Protocols
Reported In Release: FI 07.4.00	Probability: Medium

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

Defect ID: DEFECT000407438	Technical Severity: Medium
Summary: On FWS, LACP will be destroyed when the port receives LACP activity as passive, short timeout from the neighbor	
Symptom: Supposing LACP over stacking units of FCX (Unit1 and Unit2) connected with single FWS. Higher stacking priority is configured on Unti1, Unit1 is Active stacking controller and Unit2 is Standby Stacking controller in normal condition. In this condition, turning off/on power of Unit1, Unti2 to get Active stacking controller once due to switchover and then Unti2 gets reloaded after Unit1 comes up. It is an expected behavior and no problem. However during loading Unit2 until coming up, LACP status on the port of FWS that is connected with Unit1 of FCX Keeps "Inactive" status even though the port of Unit1 of FCX is "Operational" status.	
Feature: FCX L2 Control	Function: LinkAggregation - LACP/Dynamic
Service Request ID: 742619	
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000402483	Technical Severity: Medium
Summary: Flow control packets seen with no traffic on Fiber ports with 1G SFP on ICX6450/6430	
Symptom: Flow control packets (pause frames) seen with no traffic on 1G Fiber ports on ICX 6450/6430	
Feature: FI Infrastructure	Function: Flow Control
Reported In Release: FI 07.4.00	Probability: Low

Defect ID: DEFECT000410193	Technical Severity: Medium
Summary: The 'show default values' command output in ICX 6450 shows wrong max/default values for ip6-static-route and ip6-cache	
Symptom: 'show default values' in ICX6450 shows incorrect values for default and max values for ip6-static-route and ip6-cache.	
Workaround: 'show default' output should show 82 each for default and 1070 each for max values for ip6-static-route and ip6-cache.	
Feature: Layer 3 Forwarding - IPV6	Function: STATIC ROUTES (IPV6)
Reported In Release: FI 07.4.00	Probability: Medium

Open defects in Release 07.4.00

This section lists defects with High or Medium Technical Severity as of March 5, 2012. Note that when a workaround to an issue is available, it is provided; otherwise, no recommended workaround is available at this time.

Defect ID: DEFECT000380727	Technical Severity: High
Summary: TOR: DM DIag not functioning	
Symptom: DM DIag is not functioning on TI24. Command is accepted. On reboot system goes straight into App code without running diagnostics.	
Feature: Platform	Function: Dm commands
Service Request ID: 714763	
Reported In Release: FI 07.4.00	Probability: High

Defect ID: DEFECT000384408	Technical Severity: High
Summary: ServerIron HA PDUs EtherType 885a not switched across VLAN	
Symptom: The TI is dropping the SI control traffic (Ether type 885a). Ports 26 and 28 untagged in VLAN10. We can see the SI 885a packets received on 26 and 28, but they are dropped (outbound stats are 0).	
Feature: FI L2	Function: Forwarding - Other
Service Request ID: 695053	
Reported In Release: FI 07.3.00	Probability: Low

Defect ID: DEFECT000387658	Technical Severity: High
Summary: ICX6450: On rare occasions when 1Gig copper sfps are inserted to the fiber ports, the port may not come up.	
Symptom: Very rarely, when 1Gig copper sfps are inserted to the fiber ports, the port may not be operational.	
Workaround: Toggle the port state from CLI or physically hotswap the SFP.	
Feature: Platform	Function: System
Reported In Release: FI 07.4.00	Probability: Low

Defect ID: DEFECT000388641	Technical Severity: High
Summary: ICX 6430/50: Takes 3-4 minutes to release POE allocated power if there are no PDs connected or when ports go into overload state	
Symptom: When ports in the lower regions(1-30) are configured for PoE and not connected any PoE devices, it may take up to 12 minutes for powering up PDs connected to a higher port region (31-48).	
Feature: Platform	Function: Chassis - EEPROM/flash/LED/Fan/TempSensor/PSU
Reported In Release: FI 07.4.00	
Probability: Low	

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.	
Feature: SX L2 Forwarding	Function: Subnet VLAN
Service Request ID: 711367	
Reported In Release: FI 07.2.02	Probability: Low

Defect ID: DEFECT000364909	Technical Severity: Medium
Summary: DHCP Snoop data sync error	
Symptom: DHCP Snoop data sync error after hitless switchover	
Feature: FCX DHCP	Function: Client
Service Request ID: 621103	
Reported In Release: FI 07.2.02	Probability: Medium

Defect ID: DEFECT000380871	Technical Severity: Medium
Summary: Second IP fragmented packet that does not have L4 header is dropped by permit ACL	
Symptom: The problem is, one of fragmented packet is dropped by permit ACL always.	
Feature: FCX ACL	Function: ACL(all aspects of ACLs - IPV4)
Service Request ID: 692749	
Reported In Release: FI 07.2.02	Probability: Low

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
Service Request ID: 694599	
Reported In Release: FI 07.3.00	Probability: Low

Defect ID: DEFECT000383004	Technical Severity: Medium
Summary: ARP and MAC entry not updated correctly on FESX when PC removed	
Symptom: ARP and MAC entry not updated correctly on FESX when PC removed	
Workaround: After disconnecting the port, stop the ping from PC1 to PC2	
Feature: SX L2 Forwarding	Function: MAC Table/FDB Manager
Service Request ID: 695827	
Reported In Release: FI 07.3.00	Probability: High

Defect ID: DEFECT000384066	Technical Severity: Medium
Summary: In PBR the secondary gateway ip address configured is not selecting to reach the destination when the primary link is down. Its getting dropped by taking the default route.	
Symptom: The secondary gateway ip address configured is not selecting to reach the destination when the primary link is down in PBR . Its getting dropped by taking the default route.	
Feature: FCX Layer 3 Forwarding - IPV4	Function: PBR
Service Request ID: 697479	
Reported In Release: FI 07.3.00	Probability: Low

Defect ID: DEFECT000385761	Technical Severity: Medium
Summary: ICX6450/30: Output rate shaping is not accurate	
Symptom: If config rate-limit output shaping 64000kb, the actual rate will be 56400kb, not 63965kbps. There is about 10% difference. ICX6450-48 Router(config-if-e1000-1/1/48)#rate out sh 64000 Outbound Rate Shaping on Port 1/1/48 Config: 64000 Kbps, Actual: 63965 Kbps	
Workaround: Configure the rate as <Desired Rate> * 250 / 222	
Feature: FI Traffic conditioning and Monitoring	Function: outbound rate shaping
Reported In Release: FI 07.4.00	Probability: Medium

Defect ID: DEFECT000386069	Technical Severity: Medium
Summary: In ICX6450/30 PoE class is not displayed correctly for a MITEL 5360 DM phone using the command "show inline power"	
Symptom: This is only a display issue, there is no functional impact.	
Feature: Platform	Function: Chassis - EEPROM/flash/LED/Fan/TempSensor/PSU
Reported In Release: FI 07.4.00	Probability: High

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

Defect ID: DEFECT000389106	Technical Severity: Medium
Summary: ICX6450-24H Web-server frontpanel layout does not match real-life frontpanel	
Symptom: web-management frontpanel layout is inaccurate and does not match the real-life frontpanel. - Console and Mgmt ports displayed in a horizontal orientation, instead of vertically. - 10G ports are displayed in a horizontal orientation, instead of stacked 2x2. Same frontpanel image via web browser and BNA v11.1.0	
Feature: FI Embedded Management	Function: Web Management
Reported In Release: FI 07.4.00	Probability: Medium

Defect ID: DEFECT000389216	Technical Severity: Medium
Summary: OSPF adjacency not forming in standby management port	
Symptom: OSPF Adjacency not forming if it is configured on the port of the standby management module. ARP cache and IP router looks fine, ping to other end fails (no echo reply). "Show OSPF neighbor" shows the status is in EXSTART. Problem was seen in 7.2.02e and was not seen when downgrade to 4.1.00c	
Workaround: bouncing the router interface could get the OSPF neighbors to form. Rolling back to release 7.2.00 or prior can also mitigate the issue.	
Feature: OSPF	Function: OSPF
Service Request ID: 708908, 712545	
Reported In Release: FI 07.2.02	Probability: Medium