RELEASE NOTES

FastIron 08.0.80e for Ruckus ICX Switches Release Notes Version 1

Supporting FastIron 08.0.80e

Part Number: 53-1005614-01
Publication Date: 18 April 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Document History

Version	Summary of changes	Publication date
FastIron 08.0.80e for ICX Switches Version 1	Resolved issues.	April 19, 2019
FastIron 08.0.80d for ICX Switches Version 1	Resolved issues.	November 26, 2018
FastIron 08.0.80ca for ICX Switches Version 1	Resolved issue.	October 12, 2018
FastIron 08.0.80c for ICX Switches Version 1	New feature.	October 4, 2018
FastIron 08.0.80b for ICX Switches Version 1	Resolved issues.	September 5, 2018
FastIron 08.0.80a for ICX Switches Version 1	New features and resolved issues for the 08.0.80a release.	August 20, 2018
FastIron 08.0.80 for ICX Switches Version 1	New enhancements and features for the 08.0.80 release.	July 9, 2018

Introduction

About FastIron Release 08.0.80

Fastiron Release 8.0.80 introduces a number of key software features and enhancements to improve ICX switch management, usability, and scalability. This release introduces support for Ruckus SmartZone management of ICX switches, which enables SmartZone to provide monitoring, status, usage visibility, and some basic management, including configuration backups and firmware management, of ICX switches. Also introduced is a new image format called Unified FastIron Image (UFI), which combines both the Fastiron application image and boot code. New Layer 2 features include Remote Switched Port Analyzer (RSPAN) for remote mirroring. FastIron Release 08.0.80 introduces usability features such as simplified dual-mode for VLANs and increases default VLAN support and range to 1024 VLANs. This release also brings scalability enhancements in the areas of DHCP snooping, IP Source Guard, and Dynamic ARP Inspection (DAI). Another key enhancement in FastIron release 08.0.80 is the introduction of support for ICX 7650 as a cost-effective Campus Fabric (SPX) control bridge.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at ruckus-docs@arris.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The Ruckus Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

New in This Release

Hardware

There is no new hardware in FastIron Release 08.0.80.

Software Features

The following section lists new, modified, and deprecated software features for this release. For information about which platforms support these features, refer to the FastIron Features and Standards Support Matrix, available at www.ruckuswireless.com.

New Software Features in 08.0.80e

There are no new features in this release.

New Software Features in 08.0.80cd

There are no new features in this release.

New Software Features in 08.0.80ca

There are no new features in this release.

New Software Features in 08.0.80c

The following software features and enhancements are introduced in this release.

Feature	Description
SmartZone IP Address Configuration Using ICX Switch Registrar Discovery	This feature allows an ICX switch to use a DB registrar discovery mechanism to discover the list of SmartZone IP addresses.

New Software Features in 08.0.80b

There are no new features in this release.

New Software Features in 08.0.80a

The following software features and enhancements are introduced in this release.

Feature	Description
Remote Ping MIB	Remote Ping MIB was implemented as defined in RFC 4560.
Remote Traceroute MIB	Remote Traceroute MIB was implemented as defined in RFC 4560.

New Software Features in 08.0.80

The following software features and enhancements are introduced in this release.

Feature	Description
Reset CLI to factory default settings	The command triggers the factory reset action upon user accepting the reset warning message. Autocomplete is disabled for this CLI command to prevent accidental execution.
Show version for bootcode	The modified command output includes a message which warns you about any mismatch with the recommended u-boot version.
Unified FastIron Image (UFI) support	A unified FastIron image (UFI), consisting of the application image, the boot code image, and the FI signature, can be downloaded in one file. From 08.0.80, it is possible to update all the necessary software components in a setup using one command. The UFI is recommended for all image upgrades. A stack can be upgraded using a UFI bundle, and all stack members are also upgraded. The manifest Image will use the UFI to upgrade images in future releases. The manifest image will continue to use application and boot image download to downgrade to images for releases earlier than 08.0.80.The CLI for UFI image downloads will be the same as the CLI for application image downloads, except the filenames will be different.
Self-Authenticated Upgrade (SAU) licensing was implemented on all ICX7xxx platforms that run FastIron 08.0.80 or later releases.	SAU licensing, which allows a licensed feature set to be installed with a single command, was implemented for ICX 7250, ICX 7450, and ICX 7750 devices.
Ruckus SmartZone management of ICX switches	The enhancement introduces SmartZone management and monitoring of ICX switches. This initial release is the first step toward a full-featured wired/wireless integration plan and focuses on monitoring, status, usage visibility, and some basic management, including configuration backups and firmware management.
Remote Switched Port Analyzer (RSPAN)	RSPAN supports remote monitoring of multiple switches across a network. When RSPAN is enabled, a copy of each incoming or outgoing packet from one port on a network switch is forwarded to another port on the same switch where the packet can be analyzed. RSPAN can be used as a diagnostic tool for preventing network attacks. RSPAN is implemented only at the port level.
Change in default syslog buffer size	ICX devices support a local syslog buffer of up to 4,000 messages. The default value of dynamic syslog messages being logged is increased from 50 to 4,000.
HTTPS image download and configuration download/upload	HTTPS support is added for the following: • Image download to the flash over HTTPS. • Downloading a configuration file from the HTTPS server to the startup configuration file.

	• Uploading a copy of the running configuration file or the startup configuration file from a FastIron device to an HTTPS server.
Change to IPv4 ACL command	The **access-list** command has been deprecated. All instances of the **access-list** command have been replaced with the **ip access-list** command.
no-login keyword addition to the RADIUS server definition.	The keyword specifies that the RADIUS server cannot be used for login features such as TELNET, SSH, CONSOLE, EXEC, or Web-management AAA. The command allows you to designate one server for login and a different RADIUS server for NAC (including 802.1x, MAC, and Web authentication).
Flexible authentication enhancements	These Flexible authentication enhancements have been added: • Single host authentication • Multiple host authentication • Tagged VM client authentication • Information on Ruckus Vendor-Specific Attributes for RADIUS • MAC authentication support for the RADIUS user-name attribute • New configuration commands, including **auth allow-tagged enable**, **auth auth-mode**, **auth-mode**, **dot1x macauth-override**, and **mac-authentication dot1x-disable**. • New **show authentication** commands that integrate output for 802.1X and MAC authentication. and new commands for clearing authentication information: **clear authentication sessions** and **clear authentication statistics**.
ICX 7650 devices as Control Bridge (CB) units	ICX 7650 devices can be configured as a CB stack or standalone in a Campus Fabric (SPX) system. A cost-effective alternative as CB units, ICX 7650 devices have functionality equivalent to ICX 7750 CB units.
Port Extender (PE) console authentication	The console on a PE unit in a Campus Fabric network, similar to stack member behavior, redirects to the active controller console and is authenticated using the active controller CB unit user name and password.
Reconfiguring a live Campus Fabric (SPX) LAG	The **no** versions of the **multi-spx-port** and **mutli-spx-lag** command are introduced to allow SPX links to be broken on a live system. This introduces the ability to break a PE ring other than by physically disconnecting it.
Increased VLANs per PE port	By default, four VLANs are reserved per PE port, and the number of allowable VLANs per PE port is 32. The **max-vlans-per-pe-port** command is used to change the allowed number of VLANs per PE port from the default. The **max-vlans-per-pe-port** command replaces the **max-vlan** (SPX) command from this release. The **show spx-pe-port-vlan-resources** command is introduced to check related settings and resources, and the current non-default setting is displayed in **show running-config** command output.
1-Gbps Campus Fabric (SPX) links	1-Gbps SPX links are supported between ICX 7650 or ICX 7750 devices serving as CB units and connected PE units in a Campus Fabric network.
ARP inspection scale enhancements	The maximum number of static ARP inspection entries that can be configured for the entire stack has increased to 42,000.
Manifest upgrade CLI	Router and switch image can be specified for download.
Manifest upgrade (DHCP)	DHCP auto-provisioning enhancements allow overriding default behavior where the DHCP client is forced to download the application image type based on the current version of the device. The application

	image type and the flash image location can be configured as part of option 67, along with the file name.
DHCP Snooping: enable/disable DHCP option 82 at a global level	DHCP Option 82 (also known as DHCP snooping relay information) can be enabled or disabled on a VLAN or globally for all VLANs.
DHCP snooping scale enhancements	The maximum number of DHCP snooping entries that can be configured for the entire stack has increased to 32,000.
Discovery of SZ based on DHCP Option 43	DHCP option 43 can be parsed so that the SmartZone (SZ) IP address from the vendor class identifier (VCI) is received from the DHCP server and by the DHCP client as part of its request packets.
IP Source Guard scale improvements/enhancements	The maximum number of IPSG clients per port has increased to 8,000.
VLAN range command changes	The following features can be enabled on multiple VLANs with a single command: • DHCPv4 and DHCPv6 snooping • Dynamic ARP inspection • IP Source Guard • Neighbor Discovery inspection.
"Dual-mode" CLI deprecation	An interface can be added as tagged in multiple VLANs and untagged in one VLAN. No additional CLI commands are added. The interface retains its untagged VLAN membership when added as a tagged interface in another VLAN. The user can add an interface to or remove an interface from the default VLAN as an untagged member.
Increase in default system max VLANs	The default system max VLANs is increased from 64 to 1024.
VLAN and VE pre-provisioning	The enhancement allows creation of VLANS and VEs without ports so that applications can configure any feature, even before ports are added to a VLAN or VE.
VLAN range Increase	The maximum number of VLANs you can create or configure with a range command is 1024.
VLAN Mapping	VLAN Mapping provides a mechanism for Service Providers to translate CVLANs to SVLANs when a packet enters or leaves the network.
IPv6 Neighbor Discovery (ND) options	The following ND options are added: • Domain Name System Search List (DNSSL) is an IPv6 router advertisement option that allows IPv6 devices to advertise domain names of DNS suffixes to IPv6 hosts in a local area network. • Recursive DNS server addresses (RDNSS) is an IPv6 router advertisement feature that allows IPv6 devices to advertise recursive DNS server addresses and lifetime multiplier values to IPv6 hosts in a local area network. • IPv6 address advertisement suppression is an IPv6 router advertisement option that suppresses the advertisement of specified IPv6 addresses or all IPv6 addresses for router advertisement messages on an interface.
Multiple Service VLAN (SVLAN) support	A maximum of 50 SVLANs can be configured on an interface for the Q-in-Q feature.
Bridge Protocol Data Unit (BPDU) scaling	Scaling is improved for BPDU tunneling for the Q-in-Q feature.
Link Aggregation Control Protocol (LACP) timeout change without LAG flap	LACP timeout and mode changes are achieved without LAG flap.
Validation of NAC features by Cloudpath 5.2	Cloudpath release 5.2 support validation of FastIron NAC features such as 802.1X authentication, MAC authentication, Web authentication, and CoA options.
Increased number of monitor ports	The enhancement increases to 20 the number of ports that can be monitored using port mirroring or RSPAN.

Enhancement of tab-based autocomplete	When entering characters for a command or keyword that match more than one entry, you can press the Tab key to fill in the entry up to the last matching character and then enter the next unique character of the desired command or keyword to complete the entry automatically.

CLI Commands

The commands listed in this section were introduced, modified, or deprecated in FastIron 08.0.80.

New Commands in 08.0.80e

No commands were introduced or modified in this release.

New Commands in 08.0.80d

No commands were introduced or modified in this release.

New Commands in 08.0.80ca

No commands were introduced or modified in this release.

New Commands in 08.0.80c

The following commands were introduced in this release:

- **sz registrar**
- **sz registrar-list**
- **sz registrar-query-restart**

New Commands in 08.0.80b

No commands were introduced or modified in this release.

New Commands in 08.0.80a

No commands were introduced or modified in this release.

New Commands in 08.0.80

The following commands were introduced in this release:

- **auth allow-tagged enable**
- **auth auth-mode**
- **auth-mode**
- **clear authentication sessions**

- **clear authentication statistics**
- **copy https flash**
- **copy https startup-config**
- **copy running-config https**
- **copy startup-config https**
- **dot1x macauth-override**
- **ip dhcp snooping relay information disable**
- **ipv6 nd ra-domain-name**
- **ipv6 nd ra-dns-server**
- **ipv6 nd suppress-ra address**
- **license delete perpetual**
- **license set serial-number**
- **mac-authentication dot1x-disable**
- **max-vlans-per-pe-port** (SPX)
- **rspan destination**
- **rspan source**
- **rspan-vlan**
- **show authentication acls**
- **show authentication configuration**
- **show authentication sessions**
- **show authentication statistics**
- **show boot-monitor**
- **show rspan-vlan**
- **show spx pe-port-vlan-resources**
- **show sz status**
- **sz active-list**
- **sz disconnect**
- **sz disable**
- **sz query**

Modified Commands in 08.0.80c

The following command was modified in this release:

- **show sz status**

Modified Commands in 08.0.80

The following commands were modified in this release:

- **authentication max-sessions**
- **copy scp flash**

- **copy tftp flash**
- **copy tftp system-manifest**
- **crypto key client generate**
- **crypto key generate**
- **ip arp inspection vlan**
- **ip dhcp snooping vlan**
- **ipv6 dhcp6 snooping vlan**
- **ipv6 neighbor inspection vlan**
- **license delete unit**
- **license install perpetual**
- **logging buffered**
- **radius-server host**
- **show chassis**
- **show ip dhcp-client options**
- **show ip dhcp-server address-pool**
- **show license**
- **show license installed**
- **show license node-locked**
- **show license non-node-locked**
- **show license unit**
- **show logging**
- **show running-config vlan**
- **show version**
- **source-guard enable**
- **system-max max-dhcp-snoop-entries**
- **system-max max-static-inspect-arp-entries**
- **tagged ethernet**

Deprecated Commands in 08.0.80

The following commands were deprecated in this release:

- **access-list (standard numbered)**
- **access-list enable accounting**
- **access-list remark**
- **dual-mode [VLAN-ID]**
- **lldp-pass-through** (Flexible authentication)
- **max-vlan** (SPX)

RFCs and Standards

The following sections list newly supported standards and RFCs.

New Standards and RFCs in Release 08.0.80e

No new standards or RFCs are supported in FastIron Release 08.0.80e.

New Standards and RFCs in Release 08.0.80d

No new standards or RFCs are supported in FastIron Release 08.0.80d.

New Standards and RFCs in Release 08.0.80ca

No new standards or RFCs are supported in FastIron Release 08.0.80ca.

New Standards and RFCs in Release 08.0.80c

No new standards or RFCs are supported in FastIron Release 08.0.80c.

New Standards and RFCs in Release 08.0.80b

No new standards or RFCs are supported in FastIron Release 08.0.80b.

New Standards and RFCs in Release 08.0.80a

- RFC 4560

New Standards and RFCs in Release 08.0.80

No new standards or RFCs are supported in FastIron Release 08.0.80.

MIBs

The following sections list newly supported MIBs.

New MIBs in Release 08.0.80e

No new MIBs are supported in this release.

New MIBs in Release 08.0.80d

No new MIBs are supported in this release.

New MIBs in Release 08.0.80ca

No new MIBs are supported in this release.

New MIBs in Release 08.0.80c

No new MIBs are supported in this release.

New MIBs in Release 08.0.80b

No new MIBs are supported in this release.

New MIBs in Release 08.0.80a

- Remote Ping MIB
- Remote Traceroute MIB

New MIBs in Release 08.0.80

No new MIBs are supported in this release.

Hardware Support

Supported Devices

The following devices are supported in FastIron 08.0.80:

- ICX 7150 Series (ICX 7150-C12P, ICX 7150-24, ICX 7150-24P, ICX 7150-48, ICX 7150 48P, ICX 7150-48PF, ICX 7150-48ZP)
- ICX 7250 Series (ICX 7250-24, ICX 7250-24G, ICX 7250-24P, ICX 7250-48, ICX 7250-48P)
- ICX 7450 Series (ICX 7450-24, ICX 7450-24P, ICX 7450-32ZP, ICX 7450-48, ICX 7450-48F, ICX 7450-48P)
- ICX 7650 Series (ICX 7650-48P, ICX 7650-48ZP, ICX 7650-48F)
- ICX 7750 Series (ICX 7750-26Q, ICX 7750-48C, ICX 7750-48F)

Supported Power Supplies

For a list of supported power supplies, refer to the Data Sheet for your device. Data Sheets are available online at www.ruckuswireless.com.

Supported Optics

For a list of supported fiber-optic transceivers that are available from Ruckus, refer to the latest version of the Ruckus Ethernet Optics Family Data Sheet available online at www.ruckuswireless.com/optics.

Software Upgrade and Downgrade

Image File Names

Download the following images from www.ruckuswireless.com.

Device	Boot image file name	Flash image file name
ICX 7150	mnz10114.bin	SPR08080e.bin/SPS08080e.bin
ICX 7250	spz101114.bin	SPR08080e.bin/SPS08080e.bin
ICX 7450	spz10114.bin	SPR08080e.bin/SPS08080e.bin
ICX 7650	tnu10114.bin	TNR08080e.bin/TNS08080e.bin
ICX 7750	swz10114.bin	SWR08080e.bin/SWS08080e.bin

PoE Firmware Files

The following tables lists the PoE firmware file types supported in this release.

Device	Firmware version	File name
ICX 7150	2.1.0 fw	icx7xxx_poe_02.1.0.b002.fw
ICX 7250	2.1.0 fw	icx7xxx_poe_02.1.0.b002.fw
ICX 7450	2.1.0 fw	icx7xxx_poe_02.1.0.b002.fw
ICX 7650	2.1.0 fw	icx7xxx_poe_02.1.0.b002.fw

The firmware files are specific to their devices and are not interchangeable. For example, you cannot load ICX 7250 firmware on an ICX 7450 device.

NOTE
Please note the following recommendations and notices:

- Inline power is enabled by default as of FastIron release 08.0.70.
- As of FastIron release 08.0.70 **legacy-inline-power** configuration is disabled by default.
- Data link operation is decoupled from inline power by default as of FastIron release 08.0.70.
- The commands no **inline power** and **inline power** can be used to power cycle the PD.
- Data link operation is coupled with inline power using the command **inline power ethernet** *x/x/x* **couple-datalink** in Priviliged EXEC mode or in interface configuration mode using the command **inline power couple-datalink**. The PoE behavior remains the same as in releases prior to 08.0.70 (08.0.30, 08.0.40, 08.0.50, 08.0.61).
- Do not downgrade PoE firmware from the factory installed version. When changing the PoE firmware, always check the current firmware version with the **show inline power detail** command, and make sure the firmware version you are installing is higher than the version currently running.
- The PoE circuitry includes a microcontroller pre-programmed at the factory. The software can be loaded as an external file. The initial release of the microcontroller code is still current and does not need to be upgraded. 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. If a new version of the code is released, Ruckus Technical Support 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. If you encounter such an issue, please contact Ruckus Technical Support.
- PoE firmware will auto upgrade to version 2.1.0 fw during the loading of FastIron Release 08.0.80. This auto upgrade of the PoE firmware will add approximately 10 minutes to the loading of FastIron Release 08.0.80 on ICX 7150, ICX 7250, ICX 7450, and ICX 7650 devices.

Open Source and Third Party Code

Ruckus FastIron software contains or references the following third-party or open source software.

Manufacturer	Third Party Software
InMon	Sflow
Broadcom Inc	SDK 6.5.6
open source S/W	u-boot 2011.09
open source S/W	u-boot 2015.01
open source S/W	u-boot 2016.01
open source S/W	Linux 3.6.5
open source S/W	Linux 3.14
open source S/W	Linux 4.4
Aquantia Inc	Aquantia phy driver AQR API 2.1.0
Aquantia	Aquantia phy drivers: • ICX7150: AQR 3.5.E • ICX7450: AQR 2.C.5 • ICX7650: AQR 3.5.E • ICX7750: AQR 1.38.11
open source S/W	Parted utility
Broadcom Inc	Miura Phy driver 1.5

Manufacturer	Third Party Software
Broadcom Inc	EPDM driver 1.5.1
Spansion	Flash driver
http://www.bzip.org/	Bzip
http://www.hackersdelight.org/	Integer square root computation
GNU (http://www.gnu.org/)	LZMA SDK (compression method)
Freescale (NXP)	Software for PowerPC chip
Open Source SW	openssl_tpm_engine-0.4.2
Open Source SW	tpm-tools-1.3.8
Open Source SW	trousers-0.3.11.2
Infineon Technologies AG	ELTT_v1.3
Allegro Software	HTTP/HTTP-S, SSHv2
WindRiver	SNMPv1,v2c,v3; IPSecure
Interlink	Radius
SafeNet Sentinel RMS	Software Licensing Code - SafeNet Sentinel RMS
open source S/W	NSS 3.12.4 with NSPR 4.8
open source S/W	OpenSSL FIPS Object Module v2.0.5
open source S/W	OpenSSL crypto Ver 1.0.1e
GubuSoft	Javascript based tree display
GubuSoft	Javascript based tree display
GNU (The Regents of the University of California)	Syslog
BSD(The Regents of the University of California)	DNS Query/Resolution
BSD(The Regents of the University of California)	TimeZone Code (SNTP)
BSD(The Regents of the University of California)	Router Renumbering
BSD(The Regents of the University of California)	IPv6 defines
RouterWare Inc	TCP/IP stack, IPX, OSPFv2, TELNET, STP, LSL, TFTP client, BOOTP client and relay
IP Infusion	RIPng, OSPFv3, BGP4
Github	AVL Tree

Issues

Closed in Release 08.0.80e

Issue	FI-190996
Symptom	On a ICX 7650-48f stack, the standby/member deleted itself from the stack and then reloaded. After reboot the module gets struck in continuous boot loop.
Condition	On a ICX7650-48f stack, when configure "speed-duplex 1000-full" in interface range mode for standby/member, the module struck for some time and then reloaded.
Workaround	Configure the "speed-duplex 1000-full" in a smaller range of interfaces.
Recovery	Remove "speed-duplex 1000-full" configuration in standby/member and Configure the "speed-duplex 1000-full" in a smaller range of interfaces.
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	System - System

Issue	FI-187743
Symptom	When one of the power supplies is removed from a running system, the switch may reboot unexpectedly.
Condition	The system reboots when one of power supplies is removed.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.61
Technology / Technology Group	System - System

Issue	FI-191375
Symptom	Openflow controller does not communicate to ICX on management VRF
Condition	On ICX devices, enabling VRF on management interface does not communicate with openflow controller.
Workaround	No
Recovery	NA
Probability	
Found In	FI 08.0.70 FI 08.0.80
Technology / Technology Group	SDN - OpenFlow 1.3

Issue	FI-196670
Symptom	Unexpected device reload while forming SPX chains using ZTP.
Condition	SPX chain formation using ZTP with ICX7650 as CB and ICX7450,ICX7150 as PE's
Workaround	NA
Recovery	NA
Probability	Low
Found In	FI 08.0.90 FI 08.0.91
Technology / Technology Group	Stacking - Mixed Stacking

Issue	FI-186638
Symptom	When SNMP walk is done for lldpRemPortId in the Extreme switch, the output is HEX string for the interface name instead of text string.
Condition	When lldpRemPortId sub-type is configured as the value 5 (interfaceName) in ICX device and connected to the Extreme switch, the SNMP walk run in the Extreme side gives HEX string value for the interface.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.61
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-188972
Symptom	One ARP-HIPR Filter might miss in the PCL table
Condition	1. Configure BUM limit in all the interfaces to exhaust the L2 filters. 2. After reload the ARP-HIPR rule will miss in the standby PCL Table.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	Security - ACLs - Access Control Lists

Issue	FI-191475
Symptom	"show inline power" shows wrong ports as powered. Some PDs might not even power.
Condition	PoE power would be impacted on some of the ports
Workaround	None
Recovery	Upgrade to latest patch
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-189830
Symptom	Increased UFI image of size > 62MB failed tftp copy. Support for larger image has been added

Issue	FI-189830
Condition	copy tftp flash <tftp-server-ip> <image-path> primary/secondary
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-191297
Symptom	Increased UFI image of size > 62MB failed tftp copy to stack units. Support for larger image has been added
Condition	copy tftp flash <tftp-server-ip> <image-path> primary/secondary
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-191471
Symptom	Device status is not descriptive in "show inline power detail debug-info"
Condition	Better debug-ability. Added descriptive device status information in "show inline power detail debug-info" output. With this information, if the device status says "Failed" or "Lost", the unit can be RMAed.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-195159
Symptom	Sometimes ICX device is not allowing to connect incoming SSH sessions.
Condition	When large number of SSH connections happening to ICX device, sometimes SSH to ICX device fails.
Workaround	Clear the ssh sessions using kill command.
Recovery	
Probability	Medium
Found In	FI 08.0.80
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-190396
Symptom	Failure in firmware upgrade via https
Condition	Image upgrade will fail when copy is performed via https. using the command copy https flash <ip> <filename>
Workaround	None

Issue	FI-190396
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Cloud Management - Cloud Agent

Issue	FI-194684
Symptom	During scp copy of image, parallel copies corrupted the boot image.
Condition	copy scp flash <ip> <image-path> primary / secondary along with copy through multiple interfaces: console, mgmt, ssh
Workaround	Single copy at a time
Recovery	re-copy
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-184698
Symptom	Running configuration file is getting truncated while copying using scp.
Condition	Perform copy running-config scp <ip-addr> running.txt
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-195770
Symptom	Ipsec tunnel configuration is not allowed with L3-base License.
Condition	Should have l3-base license and trying to configure IPsec.
Workaround	N/A
Recovery	N/A
Probability	High
Found In	FI 08.0.80
Technology / Technology Group	Security - IPsec - IP Security

Issue	FI-185696
Symptom	In untagged VLAN open flow hybrid port for unprotected VLAN, a flow with out VLAN id gets added though its not supported.
Condition	When VLAN is configured as protected , the flow without VLAN id is accepted and installed . When the port is turned to unprotected, previously installed flow still persists.
Workaround	VLAN should not be changed from protected to unprotected mode when flow without VLAN id is configured .
Recovery	NA
Probability	

Issue	FI-185696
Found In	FI 08.0.61
Technology / Technology Group	SDN - OpenFlow 1.3

Issue	FI-191763
Symptom	Increased UFI image of size > 62MB failed tftp copy. Support for larger image has been added
Condition	copy tftp flash <tftp-server-ip> <image-path> primary/secondary will fail if the image size is greater than 62MB
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.80 FI 08.0.90
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-193916
Symptom	On ICX device, ssh session hangs sometimes without displaying prompt.
Condition	Sometimes ssh login might hang after the initial password entry.
Workaround	Retry the ssh login, and it'll succeed.
Recovery	None
Probability	
Found In	FI 08.0.80
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-191344
Symptom	“ip ospf md5-authentication” deprecated command configuration is not getting replaced by "ip ospf authentication md5 " for tunnel interface after upgrade to 8070.
Condition	"ip ospf md5-authentication" command configured on tunnel interface with ICX code version below 8070. Upgrade to 8070 and the configuration will not be displayed in the running-config and lost.
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	Layer 3 Routing/Network Layer - OSPF - IPv4 Open Shortest Path First

Issue	FI-186384
Symptom	High CPU utilization or CPU spike.
Condition	FDP enabled on a scaled 802.1BR setup with over 2200 ports.
Workaround	None
Recovery	Disabling CDP will reduce the CPU spike
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	Management - FDP - Foundry Discovery Protocol

Issue	FI-193199
Symptom	Removing a sequence from a ACL and reapplying doesn't work as expected.
Condition	Issue is seen only when ACL has multiple sequences. The sequence which is removed and re-added should be before a deny rule for the issue to occur.
Workaround	Remove and re-add entire ACL resolve's the issue.
Recovery	Remove and re-add entire ACL recover's the issue.
Probability	
Found In	FI 08.0.80
Technology / Technology Group	Security - ACLs - Access Control Lists

Issue	FI-187465
Symptom	When PBR used in network, trace-route from a host report the packet taking default route rather than PBR route.
Condition	PBR is configured on the network.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology / Technology Group	Security - PBR - Policy-Based Routing

Issue	FI-102190
Symptom	High CPU utilization due to UDP traffic destined for port 520 forwarded to CPU.
Condition	UDP traffic with destination port as 520.
Workaround	
Recovery	
Probability	Medium
Found In	
Technology / Technology Group	Layer 3 Routing/Network Layer - RIP - IPv4 Routing Information Protocol

Issue	FI-197232
Symptom	Latest PoE FW file is not available for manual upgrade.
Condition	Latest PoE FW file is not packaged.
Workaround	Get the file from TAC
Recovery	No recovery is required, FW auto upgrade is already updating the FW to latest.
Probability	Medium
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-193742
Symptom	Text "Failed to create task object for task TELNET_INCSES_1" will be displayed on session terminal. There is no functionality impact.
Condition	When NMAP port scanner script run to scan the TCP ports in ICX device. (Example: "nmap -A -v X.X.X.X")
Workaround	Stop the NMAP Port scanner.

Issue	FI-193742
Recovery	Not applicable. No Recovery Needed. There will not be any change in the device state.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-193047
Symptom	The session timeout received in access challenge packet is retained even after successful MAC-authentication/802.1x-authentication.
Condition	MAC/802.1x authentication is enabled on the interface.RADIUS server sends session timeout in access-challenge packet.
Workaround	No
Recovery	None
Probability	
Found In	FI 08.0.61
Technology / Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-189679
Symptom	"show chassis" CLI command output displays incorrect fan speed for standby and member units having single fan in their chassis.
Condition	verify "show chassis" output of a stack unit with non-active units having single fan in their chassis.
Workaround	NA
Recovery	NA
Probability	Low
Found In	FI 08.0.70
Technology / Technology Group	System - System

Issue	FI-195163
Symptom	Stack system's Active Unit might reload while establishing SSH Inbound session.
Condition	unexpected reload will be observed during SSH login to ICX box when the ICX box connecting and disconnecting to SZ (SmartZone) IP Addresss continously.
Workaround	Device can be access via Telnet sessions
Recovery	Device will reboot
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-196466
Symptom	Private vlan port is allowed to configure in regular vlan and viceversa.
Condition	Customer should have pvlan and regular vlans configured.
Workaround	N/A
Recovery	N/A

Issue	FI-196466
Probability	High
Found In	FI 08.0.80
Technology / Technology Group	Security

Issue	FI-188469
Symptom	CVE-2018-5390 - Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service. CVE-2018-5391 - The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
Condition	By sending specially crafted TCP packets within existing two-way TCP sessions.
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.70 FI 08.0.61 FI 08.0.40 FI 08.0.30 FI 08.0.80 FI 08.0.90
Technology / Technology Group	Security - Security Vulnerability

Closed with Code Change in Release 08.0.80d

This section lists software issues that were closed with code changes with Critical, High, and Medium Technical Severity in FastIron release 08.0.80d.

Issue	FI-181579
Symptom	RADIUS Accounting request for user login does not have user-name attribute.
Condition	Accounting feature with RADIUS method is enabled for user login.
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.61
Technology / Technology Group	Security - RADIUS

Issue	FI-186762
Symptom	On snmp walk , ifNumber object would display wrong value
Condition	1. Configure snmp server 2. Do snmp walk for the object IF-MIB::ifNumber.0 3. On snmp walk , ifNumber object would display wrong value
Workaround	NA
Recovery	NA
Probability	High
Found In	FI 08.0.70 FI 08.0.61
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-192117
Symptom	Code upgrade from SZ fails when 'enable telnet authentication' and TACACS+ are used together.
Condition	The issue is seen only when 'enable telnet authentication' and TACACS+ are used together.
Workaround	None
Recovery	Disable telnet authentication as a workaround
Probability	High
Found In	FI 08.0.80
Technology / Technology Group	Cloud Management - Switch Registrar/Tunnel Aggregator

Issue	FI-190300
Symptom	BGP neighbor up-time is quicker than system uptime .
Condition	When BGP is enabled BGP neighbor time is quicker than system time .
Workaround	N/A
Recovery	N/A
Probability	High
Found In	FI 08.0.61
Technology / Technology Group	Layer 3 Routing/Network Layer - BGP4 - IPv4 Border Gateway Protocol

Issue	FI-190019
Symptom	Panasonic KX-NT560 model of phone is not getting IP address.
Condition	When Panasonic KX-NT560 model of ip phone is connected to the ICX DHCP Server, the phone will not get the IP address assigned.
Workaround	N/A
Recovery	
Probability	High
Found In	FI 08.0.80
Technology / Technology Group	Management - DHCP (IPv4)

Issue	FI-190835
Symptom	Spurious syslog messages similar to the ones below are seen Oct 8 17:22:53:I:System: SSL server 192.168.11.1:443 is disconnected Oct 8 17:22:53:I:System: SSL server 192.168.11.1:443 is now connected
Condition	Only seen in FI 08.0.80c
Workaround	The command "no sz registrar" when applied as below will stop the messages Router#conf t Router(config)#no sz registrar
Recovery	None
Probability	High
Found In	FI 08.0.80
Technology / Technology Group	Cloud Management - Switch Registrar/Tunnel Aggregator

Known Issues in Release 08.0.80ca

This section lists known software issues with Critical, High, and Medium Technical Severity in FastIron release 08.0.80ca.

Issue	
Symptom	Spurious syslog messages similar to the ones below are seen Oct 8 17:22:53:I:System: SSL server 192.168.11.1:443 is disconnected Oct 8 17:22:53:I:System: SSL server 192.168.11.1:443 is now connected
Condition	Only seen in FI 08.0.80c
Workaround	The command "no sz registrar" when applied as below will stop the messages Router#conf t Router(config)#no sz registrar
Recovery	None
Probability	High
Found In	
Technology / Technology Group	Cloud Management - Switch Registrar/Tunnel Aggregator

Closed with Code Changes in Release 08.0.80b

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in FastIron release 08.0.80b.

Issue	FI-188985
Symptom	On a reload, the ICX device loses configuration for some applications. So, the configuration will not take effect in those applications.
Condition	This happens when the ICX device reloads when its configuration has Management VLAN along with other applications' configuration.
Workaround	None
Recovery	None
Probability	
Found In	08.0.80
Technology / Technology Group	

Known Issues in Release 08.0.80b

This section lists known software issues with Critical, High, and Medium Technical Severity in FastIron release 08.0.80ab.

Issue	FI-188546
Symptom	On an ICX stack or ICX SPX stack having more than one named ACLs configured or a security feature (e.g. DHCP Snooping, IP Source Guard, RA Guard etc) configured, performing a software upgrade using ISSU feature may result in either a crash during ISSU or unpredictable behavior after the ISSU is complete.
Condition	More than one named ACLs configured or a security feature (e.g. DHCP Snooping, IP Source Guard, RA Guard etc) configured
Workaround	A non-ISSU based upgrade can be used to perform software upgrade.
Recovery	None
Probability	
Found In	08.0.80
Technology / Technology Group	

Issue	FI-188203
Symptom	When either of Dynamic ARP Inspection, IPv6 Neighbor Discover Inspection and Router Advertisement Guard features are enabled on VLAN and the VLAN has ports of PE which is connected to standby unit, Upon reload of the standby unit the respective security features will not work over these ports.
Condition	Configure either of Dynamic ARP Inspection, IPv6 Neighbor Discover Inspection and Router Advertisement Guard features on a VLAN and the VLAN has ports of PE which is connected to standby unit and either the SPX reload or the standby reload or stack failover happens.
Workaround	None.
Recovery	Unconfiguring followed by re-configuring of the respective feature from the VLAN will allow the feature to work. Alternate recovery mechanism is to remove and re-add the respective PE's ports from the vlans on which the respective feature is enabled.
Probability	
Found In	08.0.70
Technology / Technology Group	

Issue	FI-188172
Symptom	In SPX ring topology when either of DHCP v4/v6 snooping, Dynamic ARP Inspection, IPv6 Neighbor Discover Inspection and Router Advertisement Guard features are enabled on VLAN and path of the PE unit to CB unit changes because of logical block movement, these features may not work for this particular PE unit. Similarly after the logical block movement, when these features are disabled on a VLAN they may continue to work.
Condition	In SPX ring topology when there is a logical block movement.
Workaround	None.
Recovery	None
Probability	
Found In	08.0.70
Technology / Technology Group	

Issue	FI-187872
Symptom	When the DHCP Clients are connected via PE which is connected to Standby Unit and when the standby unit goes for reload, the dhcp snooping will fail and the snooping database will not be populated for all those clients which are connected to this PE which is connected to standby unit.
Condition	Configure the DHCP snooping on a VLAN and the VLAN has ports of PE which is connected to standby unit and either the SPX reload or the standby reload or stack failover happens.
Workaround	None.
Recovery	Unconfiguring followed by re-configuring of DHCP snooping from the VLAN will allow the DHCP snooping entries to be populated in the snooping database for all those clients which are connected to standby unit via PE. Alternate recovery mechanism is to remove and re-add the respective PE's ports from the vlans on which DHCP snooping is enabled.
Probability	
Found In	08.0.70
Technology / Technology Group	

Closed with Code Changes in Release 08.0.80

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.80.

Issue	FI-185991
Symptom	'Broadcast limit', 'multicast limit' and 'unknown-unicast limit' configurations are accepted on PE ports but they do not work.
Condition	'Broadcast limit', 'multicast limit' or 'unknown-unicast limit' are configured on PE port.
Workaround	
Recovery	
Probability	
Found In	
Technology / Technology Group	

Issue	FI-185997
Symptom	Command link-error-disable doesn't work on lag ports
Condition	"link-error-disable " doesn't work on a lag port .
Workaround	N/A
Recovery	N/A
Probability	High
Found In	
Technology / Technology Group	

Issue	FI-186388
Symptom	After active unit resets and it comes back up and becomes active again, IPv4 routed traffic ingress on standby unit's ports are trapped to active CPU instead of hardware forwarding causing high CPU on active.
Condition	During Active/Standby synchronization of ARP/IP Cache table if switchover happens during that time the problem could be seen, thus it a corner case timing problem. It could happens with the following conditions: 1: the setup is scaled SPX or Stacking setup, (seen on SPX with 29 PE) 2: Active unit has higher priority than standby unit 3: arp table and ip cache table size is more than 1000, 4: Active unit Resets and comes back up and it automatically switch-over to active.
Workaround	Reduce the Priority of Active to be same as Standby, and if required after active resets and comes back up as Standby. Wait till on new Active message "[L3 UCAST HITLESS FAILOVER]: IPv4 Unicast hitless failover completed" is printed, then do switch over manually to make Standby becomes Active again.
Recovery	In the problem state "clear arp" on active unit can solve the issue and traffic will do hardware forwarding after re-learning of ARP.
Probability	
Found In	
Technology / Technology Group	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

Issue	FI-181850
Symptom	When there are multiple ip subnets configured on the interface, the DHCP Server might not offer the IP address from the subnet of the secondary ip addresses.
Condition	Configure a DHCP server with multi-subnet VE
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.61
Technology / Technology Group	

Issue	FI-182608
Symptom	ICX device might unexpectedly reload when the last port is removed from a LAG
Condition	Remove the last port from the LAG
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.61
Technology / Technology Group	

Issue	FI-183943
Symptom	Authentication, Authorization and Accounting of login feature like telnet, SSH, EXEC stops working after few login and logouts.
Condition	AAA is enabled for login features like telnet, SSH and EXEC.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology / Technology Group	

Issue	FI-184063
Symptom	A traceroute command to a destination succeeds but does not return the prompt (except ctrl-c) after completion.
Condition	After execution of traceroute command, it has to send ITC response notification to SSH module to release the prompt, but it sent to SNMS module. So, user needs to hit Ctrl+C to come out of the prompt.
Workaround	User can hit Ctrl+C to come out of the prompt.
Recovery	
Probability	High
Found In	FI 08.0.61
Technology / Technology Group	

Issue	FI-184066
Symptom	When IP ACL and DSCP remark commands are configured on an interface, after reload, traffic is blocked by the interface.
Condition	IP-ACL and DSCP remark commands are configured on an ve interface then traffic is blocked after reload due to wrong programming.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-185032
Symptom	While processing HTTPS, SSH, requests, occasionally system reloads due to memory leak.
Condition	Memory leak issue is observed while handling HTTPS, SSH requests.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.30
Technology / Technology Group	

Issue	FI-179167
Symptom	Sometime the Bosch camera which is a POE PD devcie does not get powered up after connecting it to ICX7150 stacking standby unit and reloading the stack. This issue happens very rarely and it is a corner case. In this case the port state mismatch is observed between stacking Active and the Standby where the Active shows port status as Down and Standby port status is shown as Up
Condition	This issue happens in a very rare case when Bosch camera PD device is connected to the ICX7150 POE port on the stacking standby unit afer the stack reload is performed
Workaround	None
Recovery	Recovery procedure is to reload the particular stacking unit or the entire stack
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-186125
Symptom	PC/Webauth Client does not get the DHCP IP address
Condition	When the uplink port is in standby/member unit of an ICX stack and it is member of a Vlan. And Admin has configured Webauth on the same vlan but has not enabled Webauth
Workaround	Enable Webauth and configure the uplink port as trust port
Recovery	Enable Webauth and configure the uplink port as trust port
Probability	
Found In	
Technology / Technology Group	

Issue	FI-185930
Symptom	IP Multicast packets with TTL=1 will hit CPU when IGMP Snooping or IPv4 PIM routing or IPv6 PIM routing is enabled.
Condition	IP Multicast packets with TTL=1 will hit CPU in following conditions 1. When IGMP snooping is enabled on those VLANs 2. When PIM routing is enabled on those network interfaces.
Workaround	If possible, increase the TTL value of the multicast stream at the source
Recovery	If possible, increase the TTL value of the multicast stream at the source
Probability	
Found In	
Technology / Technology Group	

Issue	FI-185913
Symptom	Under rare circumstances, when a stack switch-over is performed, the unit transitioning from active role to standby role crashes and boots back up.
Condition	FlexAuth is enabled and active on the system, and FlexAuth sessions are learned on ports across many Stacking and SPX units.
Workaround	None
Recovery	
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-185058
Symptom	CISCO catalyst device unable to discover ICX device in show lldp neighbor output when port-id-subtype 5 (ifName) configured on ICX.
Condition	1. lldp run on both CISCO and ICX 2. configure lldp advertise port-id-subtype 5 ports eth all on ICX side 3. show lldp neighbor on CISCO catalyst will not show ICX , neighbor discovery does not happen
Workaround	NA
Recovery	NA
Probability	
Found In	FI 08.0.61
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-184089
Symptom	Switch reloads on executing a batch buffer script on a stack setup.
Condition	A reload is triggered by executing a batch buffer script on a stack setup when the script execution leaves the CLI prompt in any mode other than PRIVILEGED EXEC mode
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.70
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-183580
Symptom	1G link is marked down when connected to a fiber port on 4x10G module of ICX7150-24P, with speed-duplex 1000-full configured on ICX7150-48ZP
Condition	1. ICX7150-48ZP connected to ICX7150-24P with speed configured to 1G. 2. Removal and insertion of 1G SFP on ICX7150-24P side makes the port down on ICX7150-24P side
Workaround	enable and disable of ICX7150-24P port brings the link up
Recovery	NA
Probability	
Found In	FI 08.0.61
Technology / Technology Group	Other - Other

Issue	FI-183100
Symptom	System resets rarely while connecting third party network monitoring tool with ICX device.
Condition	More number of HTTP, HTTPS, SSL requests polling the web management module, leads to system reset.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-109837
Symptom	SSH configuration with ACLs on the SSH access group is not working.
Condition	1. Change ssh port number: ip ssh port <xxx> 2. Configure access list: access-list <y> permit any 3. Configure access list on ssh: ssh access-group <y> 4. wr mem and reload
Workaround	
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology / Technology Group	Management - Configuration Fundamentals

Issue	FI-181239
Symptom	DHCP clients such as SONOS speakers, Ring cameras, EcoBee3 devices are not getting IP address from ICX.
Condition	When ICX device is used as DHCP server, the DHCP clients such as SONOS speakers, Ring cameras, EcoBee3 are not able to get IP address.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.61
Technology / Technology Group	Management - DHCP (IPv4)

Issue	FI-184735
Symptom	A software reset occurs on the mentioned condition
Condition	An SPX solution with DHCP snooping configured on ports of PE which is connected to standby and has a high scale of DHCP clients being updated simultaneously results in this software defect. This defect is intermittent and could happen in 1 out 5 times when such a condition exists.
Workaround	
Recovery	Reload the Ruckus ICX Switch/Router and remove the DHCP configuration from the device.
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-182302
Symptom	Although destination MAC address is correctly learned, traffic is getting flooded out on multiple ports.
Condition	When the stacking port goes down, ACL unbind is called where the port bit mask is updated for all the rules on that port.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.61
Technology / Technology Group	

Issue	FI-180143
Symptom	Unexpected reload seen in ICX stack of 1 unit
Condition	On ICX devices while trying to print buffer in console, reload occurs due to negative length value.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology / Technology Group	Management

Issue	FI-181683
Symptom	When support save all (display or tftp) command is executed, CPU spikes to 99% and data traffic is dropped
Condition	On ICX7XXX devices, supportsave all display command is triggered when flexauth dot1x is enabled.
Workaround	removing flexauth config will not create any issue in supportsave display. But this is not possible workaround for all customers.
Recovery	
Probability	Medium
Found In	FI 08.0.61
Technology / Technology Group	Management - Configuration Fundamentals

Issue	FI-182196
Symptom	When MAC-Auth succeeds and returns U:x, T:y, 2 sessions are opened with one each for Untagged and tagged VLANs (the trigger is sending tagged packets from client). Later when VLAN movement happens for updating the untagged session, the tagged VLAN session also gets updated with untagged VLAN. On subsequent receipt of tagged packets from same client, another tagged session gets created (duplicate).
Condition	Any MAC Authentication time
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.70
Technology / Technology Group	Security - MAC Port-based Authentication

Issue	FI-182899
Symptom	Security vulnerability in web server due to a script.
Condition	Security vulnerability in web server due to a script.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.30
Technology / Technology Group	Security - Security Vulnerability

Issue	FI-183753
Symptom	When reauth period and session timeout sent from RADIUS server are same values (which is generally not same, as reauth-period tend to be high and session-timeout small), 2 reauth attempts are made for the session which triggers the reauth failure from RADIUS client on the switch.
Condition	Reauth time
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.70
Technology / Technology Group	Security - MAC Port-based Authentication

Issue	FI-184384
Symptom	In FIPS-CC mode, Secure logging / Secure radius server connection establishment would fail
Condition	When device uses chain of certificates for OCSP validation to establish secure logging/secure radius server connection in FIPS-CC mode.
Workaround	Use single certificate for OCSP validation instead of chain of certificates or Remove OCSP validation For example, Below configuration has to be removed ocsp http post revocation-check ocsp ocsp-url http://10.176.166.18:2556
Recovery	
Probability	
Found In	FI 08.0.80
Technology / Technology Group	Management - AAA

Issue	FI-183964
Symptom	When 802.1X enable flag is changed from 0 to 1 during reauthentication, the session gets cleared on the local units where the session are originated from. As the control is changed from MAC-Auth to 802.1X, the session removal on the ACTIVE unit doesn't happen, which leaves the session entry. When subsequent packets hit the ACTIVE unit for MAC-Auth, as the session exists, authentication is not performed and MAC is learnt in the FDB tables.
Condition	Reauth time
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-184269
Symptom	Traffic drop due to CCEP gets blocked
Condition	Traffic drop for CCEP ingress traffic that belongs to a VLAN not running any L2 control protocols in a MCT switch.
Workaround	Reload the MCT switch
Recovery	Reload the MCT swtich.
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-181825
Symptom	Continuous reload seen when adding a new unit to the stack.
Condition	1."urpf" configured on the stack with "system-max ip-route/system-max ip6-route" set to a non-default value on the stack. 2.New unit with no running config is added to the stack. 3.New unit gets into continuous reload.
Workaround	NA
Recovery	
Probability	Low
Found In	FI 08.0.61
Technology / Technology Group	Stacking - Secure Setup, Autoconfig, Manifest files, Autocopy

Issue	FI-184093
Symptom	when user remove the vxlan overlay gateway configuration with "no overlay gateway" command, "mem L2X field VFI value does not fit" could be seen on any of active/standby/member units.
Condition	Vxlan configuration is scaled configuration with 256 vlan-vni mapping and 32 remote sites configured. And all 256 vlan are extended in every remote site. With this scale configuration when we execute "no overlay gateway" command the error/warning message could be seen.
Workaround	Workaround is to delete vxlan configuration by deleting remote sites and vlan-vni mapping separately, instead of deleting all configuration with single command "no overlay gateway".
Recovery	N/A
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-184047
Symptom	System crash while freeing the mac entry.
Condition	System configured with overlay-gateway configuration. And LAG is part of VNI mapped VLAN & some MACs are on that LAG interface. And then while deleting the LAG interface, user may see the crash.
Workaround	Before deleting the LAG interface, perform "clear mac" on LAG interface and then delete LAG interface.
Recovery	Reload the system.
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-181508
Symptom	When multiple telnet sessions are opened and multiple configuration download operations are done, system can go into a state where it continuously prints "Failed to open gpio value for reading".
Condition	When multiple telnet sessions are opened and multiple configuration download operations are done, system can continuously print "Failed to open gpio value for reading".
Workaround	Do not run multiple configuration downloads from multiple telnet sessions simultaneously .
Recovery	Reload the system to recover from this state.
Probability	High
Found In	FI 08.0.70
Technology / Technology Group	Management - IPv4/IPv6 Host Management

Issue	FI-182229
Symptom	snmp bulkwalk gives incorrect value for bgp4V2PeerDescription.
Condition	1.configure snmp-server. 2.Establish BGP connection with 4-5peers. 3.Try snmpwalk and snmpbulkwalk of bgp4V2PeerDescription. snmpbulkwalk values will be incorrect.
Workaround	NA
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-182031
Symptom	Scheduled reset from secondary in a stack boots from primary.
Condition	reload at <time> from <secondary> cli command boots from primary in a stack.
Workaround	NA
Recovery	
Probability	Medium
Found In	FI 08.0.61
Technology / Technology Group	Stacking - Traditional Stacking

Issue	FI-182122
Symptom	During Dhcp Atuo Provisioning While applying the configuration downloaded from TFTP server the remark configuration done for ACL's will be overwritten .
Condition	DHCP auto provisioning should be used to load the running configuration with multiple ACL's having remarks .
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-183203
Symptom	The RX_Power value obtained from mib browser and by running show optic command is different
Condition	Verify the show optic for that particular interface from cli and from mib browser.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-183002
Symptom	Mac from KG350s Encryptor's might not be learnt on the 7150 switches.
Condition	Send EAPOL Packet with Ethertype as 0x888e and destination mac address as 01:aa:bb:cc:00:01 from Encryptor to ICX7150.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.60
Technology / Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-181681
Symptom	User was not able do mac-authentication
Condition	When Flexauth port is disabled and then enabled again
Workaround	
Recovery	Reload the Stack
Probability	Medium
Found In	FI 08.0.61
Technology / Technology Group	Security - MAC Port-based Authentication

Issue	FI-181812
Symptom	dot1x capable PC stays in "CONNECTING" state after coming out of sleep
Condition	When PC goes to sleep and comes back, it is unable to do dot1x authentication
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-182214
Symptom	In Telnet/SSH the "show ip bgp route" command output not paged
Condition	In Telnet/SSH the "show ip bgp route" command page more is not working
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.61
Technology / Technology Group	

Issue	FI-181537
Symptom	show clock detail shows summer time start and end date incorrectly.
Condition	configure "clock summer-time" and "clock timezone us Eastern". show clock details displays incorrect start and end date for summer time
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.61
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-181728
Symptom	When stp-bpdu's are received, the interface will move to Up and Disabled state.
Condition	In ICX7250 enable stp-bpdu-guard in the interface level and when stp-bpdu's are received.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.61
Technology / Technology Group	Layer 2 Switching - BPDU Guard - Bridge Protocol Data Unit

Issue	FI-181448
Symptom	linkDown snmp trap contains unexpected value
Condition	On ICX devices, when operationally enabled port is disabled then operational status will be shown in snmp TRAP on mib browser as "Up" always. Issue seen only with snmp trap.
Workaround	No functional impact.
Recovery	
Probability	Medium
Found In	FI 08.0.30
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-181529
Symptom	Sflow collector reports XDR error.
Condition	802.1x authentication and sflow are enabled on the same interface. Sflow sends user-name attribute in the sample packet.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology / Technology Group	Security

Issue	FI-182212
Symptom	On ICX7750 stack when polled for temperature values for all the units remote units temperature will be shown as 0.
Condition	Issue is seen with ICX7750 stack when polled for temperature of remote units .
Workaround	None
Recovery	
Probability	High
Found In	FI 08.0.61
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-181963
Symptom	Configured max-reauth request value is not updated in show dot1x configuration
Condition	On ICX devices, it always shows default value for max-reauth request in show dot1x configuration even though user change it to a different value.
Workaround	No functional impact
Recovery	
Probability	Medium
Found In	FI 08.0.30
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-182216
Symptom	A software reset of the device occurs on the mentioned condition
Condition	A device with user vlan having a lag interface as a member and when webauth configuration is removed or the vlan itself is removed results in a software reset.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-182136
Symptom	show ip address output is not distinguishing between a tunnel, ve or looback interface
Condition	Configuring ip address on a tunnel or ve or loopback interface and executing show ip address. The Interface column in the output will have no distinction between tunnel or ve or loopback, their respective IDs are displayed.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.61
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-179449
Symptom	On ICX7450 switch stack when the stack failover is done then in some rare cases the port state becomes inconsistent in the output of switch CLI. For example the port could be physically up but it shows up as Down in the switch CLI output like "show interface" when this command is issued from Active or Standby unit
Condition	This issue happens rarely on ICX7450 stack when the stack failover followed by a switch over . This issue happens rarely when port is changed from untagged to tagged configuration.
Workaround	None
Recovery	Recovery procedure is to disable and enable the port, the issue does not have any functional impact.
Probability	
Found In	FI 08.0.60
Technology / Technology Group	

Issue	FI-178663
Symptom	GRE Tunnel (and potentially IP Unicast) Traffic forwarding via PE port is not getting redirected to new port even if alternative port available when PE goes down, traffic recovers when PE joins back, resulting is traffic loss even if there is alternative path.
Condition	GRE Tunnel (and potentially IP Unicast) Traffic egressing on a SPX PE Port and doing ISSU/HA operation resulting in temporary PE detach during that operation.
Workaround	Customer are advised to have PE connected to multiple CB via CB uplink spx-lag before performing switchover or failover to avoid PE Detach. For ISSU or any PE detach condition there is no workaround.
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-181603
Symptom	On ICX7650 1G copper port. When the port is configured at 100 Mbps full duplex mode and connected to link partner which is also configured at 100 Mbps full duplex mode with auto negotiation disabled. Then if the EEE (energy efficient ethernet) is enabled globally, the port goes to 100 Mbps half duplex mode.
Condition	The problem happens only when auto negotiation is disabled on the link partner and EEE configuration is enabled globally on the ICX 7650 1G port along with fixed 100 Mbps full duplex mode configuration.
Workaround	
Recovery	If a port gets into the mentioned symptom, follow the below steps for recovery. 1) “disable” the port. 2) Run the command “no eee” on the port. 3) “enable” the port.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-180921
Symptom	An error is displayed when applying an IPv6 ACL on the VE interface when there is already an existing IPv6 ACL on same interface. The error message is similar to the following message: ICX7450-24 Router(config-vif-499)#ipv6 traffic-filter scale1 in Insufficient hardware resources to apply the V6 ACL. Please remove already applied ACL(s) and/or Security features and try again. ERROR: Insufficient hardware (TCAM) resource on unit 60028 for binding the IPv6 ACL scale1 to interface 499. SYSLOG: <10> Nov 11 04:59:23 ERROR: Insufficient hardware (TCAM) resource on unit 60028 for binding the IPv6 ACL scale1 to interface 499. On the data path, the new ACL will not be programmed into TCAM and the old ACL rules still persist.
Condition	1. Configure and apply an IPv6 ACL on a VE interface 2. Now apply another IPv6 ACL on the VE interface which has logging enabled and the sizes of these two IPv6 ACLs together will exhaust the TCAM resource
Workaround	Do not enable logging on the new IPv6 ACL
Recovery	1. Remove the existing IPv6 ACL applied on the VE interface. 2. And then, apply the new IPv6 ACL on the VE interface.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-180553
Symptom	PoE powersupply is shown as regular powersupply during bootup in active unit.
Condition	Issue can be seen while executing the below set of commands. 1.clear syslog 2. reload the device 3. show log
Workaround	No Workaround
Recovery	None.
Probability	Low
Found In	FI 08.0.30
Technology / Technology Group	Monitoring - Syslog

Issue	FI-181466
Symptom	Following error messages displayed on Console/telnet/ssh: 0:_soc_mem_write_sanity_check: soc_mem_write: invalid index 87617 for memory L2_ENTRY_ONLY_ECC 0:_soc_ser_sram_correction: SER SRAM correction encoutered error(-4) in mem write
Condition	There are no specific user triggers as this is a hardware single bit error and can happen due to changes in atmosphere.
Workaround	
Recovery	Single Bit Error recovery in software automatically recovers the single bit error and error message stop after some time.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	Monitoring - OAM - Operations, Admin & Maintenance

Issue	FI-177848
Symptom	This problem happens in a scaled scenario where we have either exhausted the TCAM or adding a new filter to an ACL used for a PBR route-map will result in exhausting the TCAM resource. In this scenario, user does not get an error when adding a filter to the ACL which is used in PBR route-map. But the new filter does not get reflected in the TCAM as TCAM resource is exhausted. This applies to ACLs that are used in PBRv4 as well as PBRv6 route-maps.
Condition	Adding a filter in ACL which is used by PBR/PBRv6, when TCAM resource are exhausted or in the verge of getting exhausted.
Workaround	No workaround.
Recovery	User can add new filter after freeing up some TCAM space by deleting some existing ACL rules. The ACL rules that need to be freed up can be across any ACLs in the system and not just the ones used for PBR route-maps.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-181332
Symptom	On ICX7450 platform when the external USB is plugged in and the FIPS mode is enabled then some time the message is seen on console indicating the external USB has been plugged out "External USB-Mass-Storage Plugged-out"
Condition	
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-180871
Symptom	Duplicate packets will be received for a short window of 7 milliseconds at the device connected to this switch. Applications using Ping or any UDP based applications will report error on duplicate packet reception.
Condition	
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-181567
Symptom	On very rare occasions, during ICX7650 reload, system can encounter an unexpected kernel exception error with following message in console and not able to proceed further in the boot sequence. Sample error message: [51.081969] iproc-idm idm: idm_aci_pcie_s1 (1 21005900 358) fault
Condition	This condition was observed only when ICX7650 was reloaded back to back in a tight loop for several hours. Not seen with the normal scenarios when system is in steady state.
Workaround	None
Recovery	Reset the power for the failed unit if it is stuck in the same state.
Probability	
Found In	FI 08.0.80
Technology / Technology Group	Other - Other

Issue	FI-180631
Symptom	When scaled VXLAN overlay gateway configuration is deleted, it MAY not get deleted completely.
Condition	This issue MAY be seen when VXLAN overlay gateway (having below scaled configuration) is deleted 1. Many VLANs are mapped to VNIs i.e. more than 64 Vlan mapped to VNI 2. Multiple sites are configured i.e. more than 8 Tunnels/Sites. 3. Mapped VLANs are extended to multiple sites.
Workaround	Delete all the sites (one at a time) from the VXLAN overlay gateway, before deleting the VXLAN overlay gateway. 1). Remove site configuration one at a time. 2). This burdens CPU, so the system needs time for the CPU to come back to low, so wait for 30-60 sec for the system to settle down. Before removing next site. 3). Remove overlay-gateway in the end.
Recovery	Save the configuration and reload the switch. Once the switch boots up with partial VXLAN overlay gateway configuration, delete the VXLAN overlay gateway.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-181137
Symptom	Key used by OSPF and provisioned in key chain will be different.after Switcher/Fail over/ISSU as applications like OSPFv2/OSPFv3 that uses key-chain does not find a valid key to use for packet authentication, this may also result in adjacency flap.
Condition	When key-ids inside the key-chain are configured with expire time less than 10 seconds for all the keys and performing switch over or Fail over or ISSU.
Workaround	Key-ids inside a key-chain needs to be configured with expire time greater than 10 sec.
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-180510
Symptom	Power is not released from certain ports during back to back disconnect and connect of PDs
Condition	Power might not get released on some ports when several PDs are disconnected and reconnected in one go several times.
Workaround	Avoid disconnecting several PDs in one go. Disconnect one by one with time lag of few seconds (5 secs).
Recovery	configure "no inline power" and then "inline power" on the ports where the issue is seen.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-179153
Symptom	After the switchover, traffic policy counters on new active may not have correct values (w.r.t old active) for it's own ports.
Condition	1. There should be some traffic hitting the traffic policy before unit becomes active from standby 2. Switchover should happen at stats collection timer expiry.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-181565
Symptom	On ICX7650, if the stacking trunk is configured, and trying to do unit replacement on standby unit, could causes the protocols packet not reaching the standby unit.
Condition	This issue is observed only when stacking trunk is configured and unit replacement is done for the standby unit.
Workaround	None
Recovery	Reload the standby unit will recover from this condition
Probability	
Found In	FI 08.0.70
Technology / Technology Group	IP Multicast - IGMP - Internet Group Management Protocol

Issue	FI-108037
Symptom	The link does not come up between ICX7450-32ZP 2.5G port and ICX7750-48C 10G copper port connected using Crossover Ethernet cable with ports configured in 1G speed using "speed-duplex 1000-full-master" command
Condition	This issue happen in a connection between ICX7450-32ZP and ICX7750-48C using Crossover Ethernet cable and ports configured in 1G mode
Workaround	
Recovery	None
Probability	Medium
Found In	FI 08.0.40
Technology / Technology Group	

Issue	FI-121244
Symptom	When UDLD is enabled, LACP enabled LAG interface can flap if large ACL is applied/deleted on it.
Condition	1) UDLD must be enabled. 2) LAG should contain ports from stack member units. 3) ACL should contain more than 1000 filters.
Workaround	
Recovery	LAG interface will come back UP after the ACL programming is completed.
Probability	Medium
Found In	FI 08.0.61
Technology / Technology Group	Security - ACLs - Access Control Lists

Issue	FI-116561
Symptom	The CPU usage remains 90% for longer time when openflow controller is configured to auto download the flows and 12K flows are configured. It may cause other L2 and L3 protocol flaps.
Condition	This issue is applicable only for manual switchover cases with the highly scaled configuration and flows.
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.40
Technology / Technology Group	SDN - OpenFlow

Issue	FI-179025
Symptom	On ICX7750 when the cable is connected on the ports which are pre-configure to auto-lacp then the newly connected port comes up, goes down and then comes up again quickly. This port flap is observed only once during cable plug-in and after that the port works fine. This issue is observed only with auto-lacp and not with dynamic or static LAG
Condition	This issue is observed on ICX7750 ports when the port is configured for auto-lacp and then the cable is connected into the port to bring the link up
Workaround	There is no workaround as the port comes up after one flap and then works properly
Recovery	
Probability	
Found In	FI 08.0.61
Technology / Technology Group	

Known Issues in Release 08.0.80

This section lists open software issues with Critical, High, and Medium Technical Severity in FastIron release 08.0.80.

Issue	FI-187838
Symptom	show version CLI doesn't work. Displays an information message and returns to the prompt.
Condition	Doesn't happen easily. Happened just once in a stacking setup after 3 days of longevity, which is basically just traffic forwarding w/o any triggers or configuration changes.
Workaround	None
Recovery	None identified so far.
Probability	
Found In	
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-187670
Symptom	In multiple-untagged mode and with multiple Mac-Auth/802.1X sessions having dynamic ACLs and using the same User ACL for all sessions, any change of User ACL definitions (addition/deletion of filters in ACL) may cause high CPU usage.
Condition	With multiple sessions using the same User ACL, any filter change triggers unbinding of old filters and binding of new filters for all the sessions on that port. Depending on the number of sessions and number of filters in the User ACL, the time consumed to program ACL filters in TCAM may take significant time causing the console/telnet/ssh access to hang until the operation is complete.
Workaround	There is no workaround and the only way to prevent is not changing the User ACLs or having less number of MAC-Auth/802.1X sessions on a port and/or less number of filters in the User ACL
Recovery	There is no recovery for this symptom
Probability	
Found In	
Technology / Technology Group	

Issue	FI-187631
Symptom	The ACL show commands (e.g. show ip access-lists) display duplicate entries or missing entries when the show commands are issued from multiple sessions simultaneously.
Condition	The show commands are issued from multiple sessions simultaneously.
Workaround	None
Recovery	None
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186770
Symptom	1. When ICX is configured with a flow that should send PacketIn messages to the controller only when "no flow entries are matched", the ICX is instead sending PacketIn messages with the “reason” field set to “0” (NO_MATCH) when there is actually match with the flow entries 2. When ICX is configured with a flow that should send PacketIn messages to the controller only for packets that have matched flow entries, the ICX is sending PacketIn messages as expected but the reason code is set to “0” (NO_MATCH)
Condition	ICX is configured with a flow that should send PacketIn messages to the controller only when "no flow entries are matched" OR ICX is configured with a flow that should send PacketIn messages to the controller only for packets that have matched flow entries
Workaround	None
Recovery	None
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186891
Symptom	Telnet from ICX7150 to Cisco ASA devices fail.
Condition	Cisco ASA negotiates to use terminal type for telnet access. Terminal-type command is not supported by ICX.
Workaround	
Recovery	
Probability	
Found In	
Technology / Technology Group	Other - Other

Issue	FI-187175
Symptom	TFTP access will not be allowed in the active
Condition	Issue will be simulated with the below steps. 1. Perform stack switch over when a TFTP running configuration download is in progress (via DHCP auto provision or CLI TFTP operations). 2. Perform second stack switch over which will not allow subsequent TFTP operations on the active device
Workaround	1. Other download mechanism like SCP, HTTPS can be used. 2. The switch over can be performed when TFTP operations have completed or DHCP auto provision is complete for running configuration download.
Recovery	Reload the device or perform the third switch over operation.
Probability	
Found In	
Technology / Technology Group	Other - Other

Issue	FI-184093
Symptom	when user remove the vxlan overlay gateway configuration with "no overlay gateway" command, "mem L2X field VFI value does not fit" could be seen on any of active/standby/member units.
Condition	Vxlan configuration is scaled configuration with 256 vlan-vni mapping and 32 remote sites configured. And all 256 vlan are extended in every remote site. With this scale configuration when we execute "no overlay gateway" command the error/warning message could be seen.
Workaround	Workaround is to delete vxlan configuration by deleting remote sites and vlan-vni mapping separately, instead of deleting all configuration with single command "no overlay gateway".
Recovery	N/A
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-187052
Symptom	An ACL is getting incorrectly configured on ports of standby unit, when user tries to remove/unbind an ACL that is not bound to those standby ports.
Condition	The issue happens on stacking setup only when 1. User tries to un-configure an ACL when there is no ACL bound to that port 2. If an ACL 'X' is configured on ports of standby unit and user incorrectly tries to remove ACL 'Y' on these ports then ACL 'Y' will replace ACL 'X' on these ports.
Workaround	None
Recovery	Apply some ACL on the impacted standby ports and then remove/unbind the ACL.
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186983
Symptom	show interface brief “ displays “state” as BLOCKING for linked-up interfaces on which spanning-tree is disabled and the interface’s untagged VLAN is participating in xSTP.
Condition	Happens when spanning-tree is disabled on an interface first and then the interface’s untagged VLAN starts participating in xSTP
Workaround	Disable spanning-tree on the interface only after enabling spanning-tree in the interface’s untagged VLAN.
Recovery	Enable and disable spanning-tree on the interface after every time spanning tree is enabled on the interface’s untagged VLAN.
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186969
Symptom	ICX goes on reload , When "reload" button is submitted from web GUI while HTTPS download is in progress from CLI.
Condition	This issue occurs only with in below steps 1. Initiate a HTTPS download using the CLI command. For example: "copy https flash 10.10.10.10 icx.bin primary" 2. Open a web GUI interface for the device. 3. When HTTPS download in progress through CLI, clicks the reload button through web GUI interface
Workaround	Perform reload operation from other user interfaces or wait for download operation to complete before triggering the reload.
Recovery	NA
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186565
Symptom	if an abrupt switch over or failure open, ACL rules might not be complete if hot swap was in progress.
Condition	switch over or fail over while ACL hot swap is in progress.
Workaround	reload the units to make sure hot swap is complete.
Recovery	reload the units to make sure hot swap is complete.
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186384
Symptom	High CPU utilization or CPU spike.
Condition	CDP enabled on a scaled 802.1BR setup with over 2200 ports.
Workaround	None
Recovery	Disabling CDP will reduce the CPU spike
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186782
Symptom	it observes a crash in the active unit.
Condition	User enters erase start and reload, it observed a crash.
Workaround	none.
Recovery	after the crash, it may recover.
Probability	
Found In	
Technology / Technology Group	Stacking - Mixed Stacking

Issue	FI-186742
Symptom	Egress ACL applied on the Virtual Router Interface (VE), does not filter the traffic as per ACL rules on the PE ports of the vlan.
Condition	1. A PE port is part of more than 1 vlan 2. More than one vlan the PE port belongs have egress ACL applied on the Virtual router interface.
Workaround	If an egress ACL is to be applied on a virtual interface of a vlan with PE ports, then have the PE ports only in that single vlan. OR Apply Egress ACL on only one of the VEs the part is a member of
Recovery	1. Remove the given PE port from all the Vlans it is part of. 2. Add the PE port back to all the required vlans 3. Apply egress ACL only on one of the VEs
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186616
Symptom	Under rare circumstances, non active member of ICX7650 stack can stop showing the increments in port statistics.
Condition	Display of port statistics can stop incrementing in rare circumstances. This does not have any functional impact to the switching/routing capability.
Workaround	No workaround available.
Recovery	When ICX7650 gets into the above mentioned scenario, use "dm restart-bcm-counter" in the corresponding unit to recover from this state.
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186492
Symptom	Control packet is not forwarded from a 7450-48F (active unit). When the input is received from a member or standby unit and it RCPU the packet to a 7450-48F active.
Condition	Interpp filter outs the packet. 7450-48F have two packet processor, if the standby and member unit tries to RCPU to the active unit, the control packet comes in one packet processor and tries to forward to another port on the 2nd processor. If the output port matches the interpp filter, it will get filter out.
Workaround	This issue has to match the configuration in the topology, in this case, tries to avoid using */3/4 port because it matches the port ID of the interpp link.
Recovery	None
Probability	
Found In	
Technology / Technology Group	

Issue	FI-186518
Symptom	Console connection to CB unresponsive for 25 seconds.
Condition	End SPX PE units in a ring become unreachable causing intermediate PEs in a ring to become unreachable as well, in a scaled up SPX deployment with large number of VLANs, MACs and STP instances.
Workaround	None.
Recovery	Console becomes responsive after 25 seconds.
Probability	
Found In	
Technology / Technology Group	Layer 2 Switching - xSTP - Spanning Tree Protocols

Issue	FI-185957
Symptom	The message "INFO: all 2 display buffers are busy, please try later." will be displayed in the show command output, instead of expected functionality output. (Example show commands: "show stack", "show version")
Condition	Seen when all below conditions are met 1. The DUT is a scaled setup with huge data to display in show command 2. Two or more telnet/ssh sessions are connected. 3. The show command is performed in two sessions and output is pending for user input in the page mode in both the sessions. 4. The show command performed in the new session will show the error message "INFO: all 2 display buffers are busy, please try later."
Workaround	Abort the pending show command by pressing "Ctrl + c" in one of the two sessions or by completing the output display before performing the show command in new session. If the sessions are abruptly closed without completing the pending output, reload of the device is required
Recovery	NA
Probability	
Found In	
Technology / Technology Group	Cloud Management - Cloud Agent

Issue	FI-185679
Symptom	ACL accounting does not work for MAC filters (L2 ACLs) applied on LAG interfaces. While the statistics get collected at a per port level, the "show access-list accounting "command on lag interface does not display the accumulated statistics.
Condition	Executing a mac filter show command on a lag interface with ACL accounted enabled on MAC filters.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.80
Technology / Technology Group	Security - ACLs - Access Control Lists

Issue	FI-185437
Symptom	Clients device connected to ICX devices not being assigned an IP address (via DHCP) when the ICX device is the configured DHCP server and is in a different vlan than the client. In this scenario the DHCP server seem to allot an IP Address to the client but the client has not received the allocation.
Condition	A client device requesting an IP address through DHCP fails to receive an IP address. As a fallback mechanism it transmits a DHCP discover packet on all the vlans/ interfaces to obtain an IP address. In this condition the IP address is not allocated to the client.
Workaround	Network administrator can release IP binding for that client through a CLI command on the server. The client side configuration should be in the right vlan as a DHCP server.
Recovery	
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-181567
Symptom	On very rare occasions, during ICX7650 reload, system can encounter an unexpected kernel exception error with following message in console and not able to proceed further in the boot sequence. Sample error message: [51.081969] iproc-idm idm: idm_aci_pcie_s1 (1 21005900 358) fault
Condition	This condition was observed only when ICX7650 was reloaded back to back in a tight loop for several hours. Not seen with the normal scenarios when system is in steady state.
Workaround	None
Recovery	Reset the power for the failed unit if it is stuck in the same state.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	Other - Other

Issue	FI-185240
Symptom	IPv6 MLD snooping mcache entries are not removed from old default vlan, when the default vlan is changed.
Condition	If default VLAN is changed while Ipv6 Mutlicast traffic is received via default VLAN, IPv6 MLD snooping mcache entries related to old default VLAN is not removed from hardware. Issue seen only on switch where MLD snooping is allowed for default VLAN. This problem is applicable to all ICX products.
Workaround	Disable Multicast under default VLAN before configure/un-configure of default VLAN.
Recovery	
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-183000
Symptom	"show cli-command-history" does not display output in page mode.
Condition	"show cli-command-history" output is not displayed in page mode even after executing "page-display" command
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.61
Technology / Technology Group	

Issue	FI-184769
Symptom	ICX7450 can have an unexpected reload, when a very huge file (of the order of GBs) is copied from external USB to the unit.
Condition	Copying a very huge file (such as 1GB) from external USB to the unit can make the system busy for a longer duration. System would sense this busy condition with a watchdog timeout and will reboot automatically to recover.
Workaround	Use external USB to copy only firmware image and configuration files. These would not cause the busy condition leading to a watchdog timeout.
Recovery	System reboots and recovers itself after this unexpected
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-184384
Symptom	In FIPS-CC mode, Secure logging / Secure radius server connection establishment would fail
Condition	When device uses chain of certificates for OCSP validation to establish secure logging/secure radius server connection in FIPS-CC mode.
Workaround	Use single certificate for OCSP validation instead of chain of certificates or Remove OCSP validation For example, Below configuration has to be removed ocsp http post revocation-check ocsp ocsp-url http://10.176.166.18:2556
Recovery	
Probability	
Found In	FI 08.0.80
Technology / Technology Group	Management - AAA

Issue	FI-184378
Symptom	Ports with same configured speed will not be allowed to form a LAG as one of the below port physical characteristic didn't match, 1. Port link type is different. (Example: 1G and 10G can't form a LAG) 2. Port default speed doesn't match.
Condition	On ICX 7650 ZP and 48F platforms variants, LAG can't be formed between first 24 ports(1/1/1 to 1/1/24) and last 24ports (1/1/25 to 1/1/48) even though the configured speed is same.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-184003
Symptom	The key/certificate generation performed when a previous key/certificate generation command is still in progress, would fail with error message "A key pair generation is already in progress..."
Condition	When ssl certificate/ssh key generation command is performed during the previous ssh key/ssl certificate generation is in progress. Example commands for ssh key and ssl certificate generation: ssl certificate: "crypto-ssl certificate generate" ssh key: crypto key generate rsa modulus 2048 This scenario would be possible during config download if the configuration fie has both the key generation commands.
Workaround	Perform the next ssl certificate/ssh key generation command after the previous key/certificate generation command completes.
Recovery	Reexecute the key/certificate generation command.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-183122
Symptom	PIM Mcache (show ip pim mcache) will continue to show the old OIF(Port) that got converted into Lag, with no impact on HW forwarding.
Condition	This is seen when a OIF Port is part of the PIM Mcache is converted into Lag or vice versa by configuration change.
Workaround	
Recovery	Execute the command "Clear ip pim mcache" to clear the mcache. But this will have traffic impact for the existing flow.
Probability	High
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-177848
Symptom	This problem happens in a scaled scenario where we have either exhausted the TCAM or adding a new filter to an ACL used for a PBR route-map will result in exhausting the TCAM resource. In this scenario, user does not get an error when adding a filter to the ACL which is used in PBR route-map. But the new filter does not get reflected in the TCAM as TCAM resource is exhausted. This applies to ACLs that are used in PBRv4 as well as PBRv6 route-maps.
Condition	Adding a filter in ACL which is used by PBR/PBRv6, when TCAM resource are exhausted or in the verge of getting exhausted.
Workaround	No workaround.
Recovery	User can add new filter after freeing up some TCAM space by deleting some existing ACL rules. The ACL rules that need to be freed up can be across any ACLs in the system and not just the ones used for PBR route-maps.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-113814
Symptom	Currently the system is allowing the user to configure PBR on the same interface where FlexAuth is also enabled and the user configured RADIUS to apply ACL on the FlexAuth session. Traffic forwarding is nondeterministic due the order in which the access list rules are configured on member units when PBR and dynamic ACLs are configured on the same interface.
Condition	This happens when user configures PBR on the same interface where FlexAuth is also enabled and the user configured RADIUS to apply ACL on the FlexAuth session. It is not a recommended way to use the system.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.61
Technology / Technology Group	Security - PBR - Policy-Based Routing

Issue	FI-181286
Symptom	User might see i2c error messages displayed in console when plugging in or when accessing an unsupported SFPP. Sample error message: I2C_CORE: B80:D51 Read Failed.Bytes read=0 Bytes to read=1.
Condition	User might see i2c related error messages, when plugging in an unsupported SFPP. This was observed on SFPP with part name: AFBR-707ASDZ-BR2
Workaround	Please use only supported SFPP.
Recovery	Replace any unsupported SFPP in the unit with a supported one.
Probability	
Found In	FI 08.0.70
Technology / Technology Group	Other - Other

Issue	FI-123259
Symptom	Pre-provisioned ACL configurations that applies to a PE are not properly applied on that PE during hotswap.
Condition	Filters of one or more ACLs that belong to pre-provisioned ACL configurations that apply to the PE being hotswapped, are assigned new sequence numbers through 'resequence' command while the PE hotswap is in progress.
Workaround	Do not attempt to resequence the filters of any ACLs while any PE hotswap is in progress. Check SYSLOG for messages regarding the ongoing and completion related messages for PE hotswaps for making the decision.
Recovery	Reload the affected PE.
Probability	Medium
Found In	FI 08.0.50
Technology / Technology Group	Security - ACLs - Access Control Lists

Issue	FI-116781
Symptom	A binding of ACL using filters matching one or more ranges of TCP/UDP ports to ports of a member unit fails due to TCAM rules unavailability.
Condition	The ACL (using filters matching one or more ranges of TCP/UDP ports) that is bound to ports of member units is bound "after" several ACLs using filters matching one or more ranges of TCP/UDP ports are already applied to ports of Active unit.
Workaround	Apply the ACL (using filters matching one or more ranges of TCP/UDP ports) to ports of member units "before" applying any ACLs using filters matching one or more ranges of TCP/UDP ports are applied to ports of the Active unit.
Recovery	Unbind all ACLs (using filters matching one or more ranges of TCP/UDP ports) that are bound to the ports of the Active unit, and then attempt to apply the ACL (using filters matching one or more ranges of TCP/UDP ports) to ports of member units.
Probability	Medium
Found In	FI 08.0.60
Technology / Technology Group	Security - ACLs - Access Control Lists

Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com