RELEASE NOTES

FastIron 08.0.91 for Ruckus ICX Switches Release Notes Version 1

Supporting FastIron 08.0.91

Part Number: 53-1005593-01
Publication Date: 28 June 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..4

Introduction..4

About FastIron Release 08.0.91..4

Document Feedback..4

Ruckus Product Documentation Resources..4

Online Training Resources..5

Contacting Ruckus Customer Services and Support..5

New in This Release..6

Hardware 6

Software Features..7

CLI Commands..7

RFCs and Standards..7

MIBs 7

Hardware Support..8

Supported Devices 8

Supported Power Supplies..9

Supported Optics..9

Software Upgrade and Downgrade..9

Image File Names..9

PoE Firmware Files..9

Open Source and Third Party Code..10

Issues..12

Closed with Code Changes in Release 08.0.91..12

Known Issues in Release 08.0.91..21

Document History

Version	Summary of changes	Publication date
FastIron 08.0.91 for ICX Switches Version 1	• Added three ICX 7150 SKUs: ICX 7150-C08P, ICX 7150-C10ZP, ICX 7150-24F • Resolved issues	June 28, 2019

Introduction

About FastIron Release 08.0.91

FastIron release 08.0.91 introduces new additions to the ICX7150 switch product line. The ICX 7150-24F provides 24 ports of 1GbE SFP, and up to 4 ports of 10GE SFP+. The ICX 7150-C10ZP provides 10 ports of Multigigabit Ethernet, and 4 ports of 95W PoE. The ICX 7150-24F and ICX 7150-C10ZP supports L2 switches and L3 advanced routing features, up to 12 unit stacking, Campus Fabric support, and SmartZone manageability. The ICX 7150-C08P provides 8 ports of 1GbE PoE and 2 ports of 1GE SFP uplinks. The ICX 7150-C08P supports L2 switches features, and is designed for standalone operation, and SmartZone manageability.

FastIron release 08.0.91 also introduces support for automation with Ansible, and Energy Efficient Ethernet (EEE) support on the ICX 7150.

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

The following section lists new hardware introduced with this release and hardware that is no longer supported with this release.

New Ruckus ICX 7150 Switch SKUs

FastIron release 08.0.91 introduces three additions to the ICX7150 switch product line.

The ICX 7150-24F supports the following:

- 24 ports of 1GbE SFP
- up to 4 ports of 10GE SFP+
- L2 switching features
- L3 advanced routing features
- up to 12 unit stacking
- Campus Fabric support
- SmartZone manageability

The ICX 7150-C10ZP supports the following:

- 10 ports of Multigigabit Ethernet
- 4 ports of 95W PoE
- L2 switching features
- L3 advanced routing features
- up to 12 unit stacking
- Campus Fabric support
- SmartZone manageability

The ICX 7150-C08P supports the following:

- 8 ports of 1GbE PoE
- 2 ports of 1GE SFP uplinks
- L2 switching features
- SmartZone manageability

Deprecated Hardware

The ICX 7750 Campus Switch is no longer supported beginning in FastIron Release 08.0.91. The ICX 7750 will continue to be supported in the FastIron 8.0.90 release stream.

Software Features

The following section lists new, modified, and deprecated software features for this release.

New Software Features in 08.0.91

The following software features and enhancements are introduced in this release. Refer to the FastIron Features and Standards Support Matrix, available at www.ruckuswireless.com, for a detailed listing of feature and platform support.

Feature	Descriptions
Automation with Ansible	Ansible can be used to set up automation and configuration management of ICX switches. Ansible support for the Ruckus ICX series of product can be found at https://docs.ansible.com/ansible/latest/modules/list_of_network_modules.html#icx
EEE support on the ICX 7150	Support for Energy Efficient Ethernet is added to the ICX 7150.

CLI Commands

The commands listed in this section were introduced, modified, or deprecated in FastIron 08.0.91.

New Commands in 08.0.91

No new commands have been introduced in 08.0.91.

Modified Commands in 08.0.91

- **ip ssh idle-time**

Deprecated Commands in 08.0.91

No commands have been deprecated in 08.0.91.

RFCs and Standards

There are no newly supported RFCs or standards in release 08.0.91.

MIBs

There are no new MIBs in release 08.0.91.

Hardware Support

Supported Devices

The following devices are supported in release 08.0.91.

- ICX 7150 Series (ICX 7150-C08P, ICX 7150-C10ZP, ICX 7150-C12P, ICX 7150-24, ICX 7150-24F, 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 7850 Series (ICX 7850-32Q, ICX 7850-48FS, ICX 7850-48F)

Default Username and Password

Note that new ICX switches that are initially deployed using 08.0.90 or later releases must be accessed using the following default local username and password:

- Default local username: super
- Default password: sp-admin

The default username and password apply to all forms of access including Console, SSH and WEB2. The administrator will be prompted to create a new password after logging in. ICX devices that are already deployed with a previous release and upgraded to 08.0.90 will not be affected by this change.

Deprecated Devices

Beginning in release 08.0.91, the following devices have been deprecated:

- ICX 7750 Series (ICX 7750-26Q, ICX 7750-48C, ICX 7750-48F)

Note that the ICX 7750 Switch will continue to be supported in release 08.0.90.

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.

The UFI (which was introduced in 08.0.80) consists of the application image, the boot code image, and the signature file, and can be downloaded in a single file.

Beginning with FastIron 08.0.90, any new ICX hardware platform (starting with the ICX 7850) will use only UFIs. Any systems upgraded from 08.0.70 or earlier releases directly to 08.0.90 manually or using the manifest file must be upgraded a second time using the UFI image. If the upgrade is from 08.0.80, then use the UFI image.

Device	UFI file name (boot, image)
ICX 7150	SPR08091ufi.bin/SPS08091ufi.bin
ICX 7250	SPR08091ufi.bin/SPS08091ufi.bin
ICX 7450	SPR08091ufi.bin/SPS08091ufi.bin
ICX 7650	TNR08091ufi.bin/TNS08091ufi.bin
ICX 7850	TNR08091ufi.bin

PoE Firmware Files

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

Device	Firmware version	File name
ICX 7150	2.1.1 fw	icx7xxx_poe_02.1.1.b002.fw
ICX 7250	2.1.1 fw	icx7xxx_poe_02.1.1.b002.fw
ICX 7450	2.1.1 fw	icx7xxx_poe_02.1.1.b002.fw
ICX 7650	2.1.1 fw	icx7xxx_poe_02.1.1.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.
- Use the **[no] inline power** command to enable and disable POE on one or a range of ports.
- 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 microcontrollers are pre-programmed at the factory. The firmware can be loaded as an external file. 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.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 6.5.13
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 OS: • ICX7150, ICX7250, ICX7450: Linux 4.4 • ICX7650, ICX7850: Linux 3.14.65
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
open source S/W	Parted utility
Broadcom Inc	Miura Phy driver 1.8
Broadcom Inc	EPDM driver 1.7.4

Manufacturer	Third Party Software
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
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
open source S/W	libunwind
Wind River Systems, Inc.	Wind River MIB Compiler, version 10.2

Issues

Closed with Code Changes in Release 08.0.91

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.91.

Issue	FI-198096
Symptom	Mac-Authentication Traps are not generated.
Condition	When the Mac-Auth Interface is in non-active unit, traps are not generated
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-197396
Symptom	On ICX device, web authentication will fail when username and password length is given more than 32 characters.
Condition	When user enters credentials more than 32 characters for web authentication it will fail.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-197616
Symptom	Active unit of the stack reloads unexpectedly when console to member units.
Condition	When console to any of the member units in a 7 or more units stack, the active unit reloads after few minutes.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-197061
Symptom	Ocassionally, when the SCP script is run in the background to backup the running Config of ICX device, access to flash will be denied for 20 minutes.
Condition	User will receive the message "Flash access in progress. Please try later" when issuing 'write mem' and if SCP script is run in the background to backup the running Config.
Workaround	NA
Recovery	NA
Probability	Low
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-197402
Symptom	When connected to the member unit console, cannot get into the enabled mode.
Condition	When consoled into any of the member units in a 7 or more units stack, enabled mode is not allowed.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-197128
Symptom	Occasionally, 'show flash' command shows the primary and secondary image files are empty and flash free space is zero.
Condition	'show flash' CLI command output shows the primary and secondary image files are empty and flash free space is zero.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.70
Technology / Technology Group	System - System

Issue	FI-197358
Symptom	The member units in a stack reloads unexpectedly.
Condition	When MAC notification is enabled, sometimes the member units in a stack reloads unexpectedly due to memory leak.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-195770
Symptom	In Fastiron 08.0.80 code, the IPSEC commands are not available and asked for L3 premium license.
Condition	In Fastiron 08.0.80 code, the IPSEC commands are not available until L3 premium license is installed.
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.80
Technology / Technology Group	Security - IPsec - IP Security

Issue	FI-196211
Symptom	show cpu reports 8% CPU for 1 sec average infrequently in ICX 7150. No known functional impact.
Condition	CPU usage monitoring when done with sh cpu
Workaround	None
Recovery	CPU utilization comes back to normal levels after the spike
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

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-191652
Symptom	Crash is seen when IPV6 client is trying to get an IP address from dhcpv6 server with dhcpv6 snooping enabled.
Condition	Issue is seen only when Dhcpv6 snooping is enabled and client is getting IP address from the server .
Workaround	N/A
Recovery	N/A
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-194094
Symptom	In SPX setup, CB unit might reload unexpectedly after several days of uptime.
Condition	If we trigger a scp script when there is a configuration change in the SPX set-up to copy running-config from device to scp server .
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	Layer 2 Switching - Switch Port Extender

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-193353
Symptom	IPv6 Route table full and IPv4 route table Full error messages would be printed in console.
Condition	1. Configure reverse-path-check. 2. Ping or tcp/udp scan an IPv6 subnet on ICX7K device to add more than 1024 IPv6 routes.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-196247
Symptom	Cloudpath Webauthentication doesn't work after reload if trust port Lag is applied for webauth
Condition	when Reloaded
Workaround	Remove and add "trust port lag" from webauth configuration
Recovery	Remove and add "trust port lag" from webauth configuration
Probability	
Found In	FI 08.0.70
Technology / Technology Group	Security - Web Authentication

Issue	FI-196484
Symptom	Mac-Authentication Syslog's and Traps are not generated
Condition	Syslog's and Traps are not generated in the following scenarios 1. Mac-Authentication failure due to Access Reject from Radius. 2. Mac-Authentication Success 3. Mac-Authentication Radius Timeout
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.80 FI 08.0.90
Technology / Technology Group	

Issue	FI-196530
Symptom	Show stack discover neighbor command make the switch to reboot
Condition	when the cli "show stack discover neighbor" is executed.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	Cloud Management - Cloud Agent

Issue	FI-196322
Symptom	On rare occasions, the statistics of stacking ports are displayed as zero. This was observed only on Megamind Units during SQA testing.
Condition	This issue was observed only on MM units.
Workaround	Reboot of the system should fix the issue.
Recovery	
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-196515
Symptom	This is an additional SYSLOG message. This also prints certain stack traces during reload events and RADIUS shared secret key additions and updates.
Condition	The SYSLOGs and the traces are printed during the reload events and share secret key changes. They look similar to SYSLOG: <118>Jan 1 00:00:26 6450_U40 stack: 01988018 01855a90 018565a4 019dda78 019de788 0176da28 016d8c84 022946ac 02fccb28 SYSLOG: <118>Jan 1 00:00:26 6450_U40 stack: 01988018 01855a90 018565a4 019dda78 019de788 0176da28 016d8c84 022946ac 02fccb28 SYSLOG: <118>Jan 1 00:00:26 6450_U40 stack: 01988018 01855a90 018565a4 019dda78 019de788 0176da28 016d8c84 022946ac 02fccb28
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.70 FI 08.0.30
Technology / Technology Group	Security - AAA - Authentication, Authorization, and Accounting

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 and 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-196064
Symptom	The edge devices will not be able to get through MAC/Dot1x authentication process.
Condition	This could happen when RADIUS server does not send response or sends the response with invalid key.
Workaround	None.
Recovery	Clear the entries using the command, clear radius radius-queue
Probability	Medium
Found In	FI 08.0.70 FI 08.0.30
Technology / Technology Group	Security - MAC Port-based Authentication

Issue	FI-196158
Symptom	ICX switch may reload when making configuration changes to LAG configuration.
Condition	The conditions in which the issue is occurring is not evident. This issue can happen under rare scenarios.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.70
Technology / Technology Group	Layer 2 - Link Aggregation

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-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.
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-195054
Symptom	Optical Monitoring is not working for 1G M-LHA(SFP)
Condition	Issue is seen only with SFP types 1G M-LHA(SFP) Part# : 57-0000194-01
Workaround	N/A
Recovery	N/A
Probability	Medium
Found In	FI 08.0.30
Technology / Technology Group	System - Optics

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-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-194289
Symptom	LRM support is same as 8.90 release. Following changes in the port with LRM optic may flap the other ports in the same PHY: 1. Changing speed from 10G to 1G 2. Plugging out optic
Condition	LRM optic on 10G ports (ICX7850-48FS module 1 ports)
Workaround	None
Recovery	interfaces automatically comes up after the flap.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Other - Other

Issue	FI-192622
Symptom	In a scaled setup with 12 unit stack, if user tries to unconfigure all, telnet session can be timeout.
Condition	unconfigure the stack in a scale setup
Workaround	reconnect to the telnet session when the timeout happen.
Recovery	reconnect to the telnet session when the timeout happen.
Probability	High
Found In	FI 08.0.90
Technology / Technology Group	Stacking - Secure Setup, Autoconfig, Manifest files, Autocopy

Issue	FI-195139
Symptom	On an ICX device, when a packet does not match an ACL rule which looks for a DSCP/802.1p value and if the packet comes to slow path, the packet gets forwarded in the slow path due to the same rule even though it logically matches with a deny rule below that.
Condition	This issue happens when the packet matches with another rule that has logging configured. For example, in the following case the deny rule has log enabled. ipv6 access-list ipv6: 2 entries enable-accounting logging-enable 20: permit any any log dscp-matching 11 30: deny ipv6 any any log
Workaround	Avoiding the "log" option on filter while using a permit rule with match by DSCP.
Recovery	No Recovery
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-192315
Symptom	Stack Device reboots, executing "show ip pim mcache" with filter enabled for large number of PIM entries.
Condition	Stack Device having 2000+ PIM entries, will reboot while executing below sequence of show commands in console session. 1. execute "show ip igmp group" and Press Ctrl+c at page mode 2. execute "show ip pim mcache" and Press Ctrl+c at page mode 3. execute "show ip pim mcache | include 2000" and Press Ctrl+c.
Workaround	Use Telnet or SSH sessions to perform these operations.
Recovery	NA
Probability	
Found In	FI 08.0.90
Technology / Technology Group	IP Multicast - PIM - Protocol-Independent Multicast

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-195030
Symptom	A momentary high CPU for upto 2 seconds can be seen during write memory when changing boot sequence
Condition	Changing the default boot sequence and doing a write memory can cause a momentary high CPU (for upto 2 seconds)
Workaround	No workaround available. User may choose to boot from other partition using CLI instead of setting it in configuration.
Recovery	No need for any recovery as the systems recovers automatically from the momentary high CPU
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-193290
Symptom	When mode button is pressed in ICX7850, there could be a few seconds of latency for the port LEDs to get updated
Condition	Pressing mode button can cause the LED update is delayed by few seconds
Workaround	
Recovery	No recovery needed. LED gets updated automatically after few seconds
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-194675
Symptom	The rate at which MAC addresses are learnt in ICX7850 platform is lower than ICX7750 platform by 35%. Due to this the customer could see increased flood traffic in the network for additional time.
Condition	Arrival of traffic with new MAC addresses at a rate above 1300 packets/sec to an ICX7850 unit.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Layer 2 Switching

Issue	FI-191518
Symptom	In ICX DHCP Server running with the switch image, the clients are not assigned with the dynamic IP address.
Condition	When the clients are connected to ICX DHCP Server in non-default VLAN or non-management VLAN, then the clients are not assigned IP address.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70 FI 08.0.80
Technology / Technology Group	

Known Issues in Release 08.0.91

This section lists open software issues with Critical, High, and Medium Technical Severity in FastIron 08.0.91.

Issue	FI-199495
Symptom	The ports link status shows down after coverting from stacking to uplink ports
Condition	Problem description: Ø When stack unit is converted from Ring to Linear, the port/s may remain down (As of now the issue is observed only with 2PP devices) Ø When stack unit is converted from Linear to Ring, the port/s may go down (observed very rarely)
Workaround	
Recovery	Ø After converting stack from Ring to Linear, disable and enable the concerned data ports o interface eth x/y/z o disable and enable the interfaces Ø After converting stack from Linear to Ring, reload the units where stack configuration is performed Ø reload units x,y
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-199493
Symptom	Momentory traffic drop on member units while converting the stack topology from Ring to Linear
Condition	Problem description: When a stack unit is converted from Ring to Linear, there will be a momentary flood of BUM traffic in newly converted data/uplink ports and traffic may be affected.
Workaround	How to avoid this issue: Ø Before converting stack from Ring to Linear, Disable FDP – “no fdp run” and re-enable after all conversion is taken place
Recovery	Ø Convert stack from Ring to Linear “no multi-stack-port x/y/z and a/b/c” Ø Disable and Enable STP on newly created data port o interface eth x/y/z eth a/b/c o no spanning o spanning
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-199243
Symptom	Ping failed between member and active after removing link from ring topology
Condition	Problem description: When a 7150 stack unit is converted from Ring to Linear using CLI "no multi-stack-trunk or no multi-stack-port", communication between the units may fail and user may experience drop while traffic flowing across the stack. The problem can be seen in “show stack connection” output where “*** Error! only one directional CPU to CPU:” will be seen if the problem occurs. ICX7150-48P Router# show stack connection active standby +---+ +---+ +-+ | 5 |3/1--3/1| 1 |3/3--3/2| 4 | +---+ +---+ +---+ probe results: 2 links, P0/1: stk-port dir 0/1, T0/1: stack-trunk dir 0/1 Link 1: u1 -- u5, num=1 1: 1/3/1 (P0) <---> 5/3/1 (P0) Link 2: u1 -- u4, num=1 1: 1/3/3 (P1) <---> 4/3/2 (P0) *** Error! only one directional CPU to CPU: u4 --> u1 This issue can be seen in two scenario’s: Ø Scenario 1: o If the link is unconfigured using “no multi-stack-port" in the stack. Ø Scenario 2: o If the link is unconfigured using “no multi-stack-trunk" in the stack for the stack trunk links.
Workaround	Avoiding issue: Ø To avoid this issue, User can convert the stack from “Ring” to “Linear” topology by removing the stack link physically. Ø Remove the stack configuration from running configuration
Recovery	Recovery issue: Ø If problem occurs, reload the entire stack.
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-199314
Symptom	Management port not forwarding packets more than 1500 bytes when system has Jumbo packets enabled in any of the forwarding ports.
Condition	MTU size greater than 1500 in Management port
Workaround	Disable Jumbo packets if Management port needs to fragment packets more than 1500 bytes
Recovery	Packet size in the management plane should be restricted within the supported 1500 bytes
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-199245
Symptom	High CPU followed by watchdog timeout and crash will be observed in SPX CB units.
Condition	Issue happens only on CB units with large number of ports in default VLAN when STP is disabled in the default VLAN.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-198891
Symptom	When an IP-Sec module is present in the ICX-7450 unit, the Digital and Optical Monitoring stops working even when its configured on the unit.
Condition	The IP-Sec module must be present in the ICX-7450 unit to observe this issue.
Workaround	The removal of IP-Sec module resumes the DOM (Digital and Optical Monitoring) operation.
Recovery	The resolution for this issue shall be provided in the next release.
Probability	
Found In	FI 08.0.90 FI 08.0.91
Technology / Technology Group	

Issue	FI-198851
Symptom	Incoming traffic from IPSG Client IP's on ICX switch/router will not be honored if and only if the IP's learnt are from the Standby unit port where IPSG is enabled on physical or plain interface.
Condition	On ICX Switch/Router Enable IPSG on Standby unit physical port.
Workaround	
Recovery	No Recovery.
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-197681
Symptom	owner configuration under VRRP instance cannot be removed by running "no owner" command. Owner configuration will be retained.
Condition	This can be seen when 'no owner' is done under vrrp instance
Workaround	There is no need of removing the owner configuration. if required it can be modified by setting it to backup mode. The role of vrrp instance can either be owner or backup.
Recovery	Recovery is not applicable here. This has no functionality impact.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Layer 3 Routing/Network Layer - VRRPv3 - Virtual Router Redundancy Protocol Version 3

Issue	FI-198197
Symptom	Class attribute is present in all AAA accounting packets sent by all authenticated Users
Condition	When class attribute is sent by Radius Server in AAA-ACCEPT message for a single User during authentication and there are more than one authenticated User in FI Switch/Router
Workaround	There is no workaround
Recovery	Reset the class attribute in the Radius Server and then reload the FI Switch/Router
Probability	
Found In	FI 08.0.90 FI 08.0.92
Technology / Technology Group	

Issue	FI-198665
Symptom	SYSLOG: <11> Jan 1 21:13:17 DHCP6: ITC proc_boot_msg (action start) send failed to hmon Error in sending message to hmon, ITC return code: 17
Condition	When DHCPV6 is configured FastIron process sends a ITC message to hmond to start dhcp daemon, and if hmond process is not running the dhcp daemon start will fail, along with that ITC failure messages will be printed on the console
Workaround	The cause for failure is yet to be root-caused, hence there are no workarounds now to prevent the switch from hitting this issue
Recovery	There are no workarounds to start hmond on the fly, however the issue can be mitigated by moving the Active role to another unit in the stack, since hmond will be running on the node which became 'new Active' DHCPV6 will be started on the new Active.
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-198427
Symptom	RSTP state for a particular port shows up as "BROKEN" in a scenario where UDLD is configured ONLY on one side of the link.
Condition	The issue is seen ONLY if as long as UDLD is configured on one side of the link.
Workaround	When UDLD is configured on both sides of the link, the issue wont be observed.
Recovery	When UDLD is configured on both sides of the link, the issue wont be observed.
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-195864
Symptom	Tanto box hits watchdog timeout after 9-14 days.
Condition	It is observed if macsec data is pumped through front ports and plug-in module ports at line rate and stack switchover is done after 7-9 days.
Workaround	No workaround.
Recovery	Box reboots after core collection.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Other - Other

Issue	FI-198291
Symptom	On failover of Active, the rconsole of PE return to its local session.
Condition	Failover of a two unit stack with PE connected to standby
Workaround	NA
Recovery	Do a rconsole to active from PE.
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-198271
Symptom	BUM Suppression configuration get applied even though Insufficient Hardware resource Error is thrown.
Condition	No available TCAM Resource.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-197960
Symptom	BGP and OSPF SNMP traps doesn't contain human readable strings in the description field
Condition	Any MIB browser which has the "description" field will display non-readable strings when BGP and OSPF traps are generated by the ICX device.
Workaround	NA
Recovery	NA
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-197083
Symptom	Multicast Host will not receive the traffic from its IPv6 PIM designated router (DR), if there is another PIM router in the same VLAN which is the upstream router for the multicast source.
Condition	This problem is specific to the IPv6 PIM-SM. If multicast host (receiver) is connected to a VLAN, in which the PIM DR router (say R1) is also the RP(Rendezvous Point) and the upstream router for the source is another router (say R2). In this topology, the multicast host will not receive the traffic, if R1 has no other receiver.
Workaround	none
Recovery	Use the CLI command "ipv6 pim dr-priority <val>" to adjust the designated router(DR) priorities such that upstream PIM router(R2) becomes the DR.
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-196776
Symptom	User may not see advertised capabilities in ICX7150-C10ZP for the CLI: show lldp local-info
Condition	When user issues a command show lldp local-info on C10ZP, the advertised capabilities of the port may not be displayed.
Workaround	No workaround available
Recovery	No recovery needed, since the autoneg works fine. It is only a display issue.
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-196211
Symptom	show cpu reports 8% CPU for 1 sec average infrequently in ICX 7150. No known functional impact.
Condition	CPU usage monitoring when done with sh cpu
Workaround	None
Recovery	CPU utilization comes back to normal levels after the spike
Probability	
Found In	FI 08.0.91
Technology / Technology Group	

Issue	FI-185144
Symptom	On an ICX 7K stack, if a packet having Invalid Source Module ID in the Higig header enters the stack link, it will keep looping within the stack.
Condition	By design, all the packets sent over the HiGig links are initialized with valid Source Module ID. It is not known at this point any specific sequence of steps that lead to the Source Module ID becoming invalid.
Workaround	no workaround
Recovery	None
Probability	
Found In	FI 08.0.70 FI 08.0.61 FI 08.0.60 FI 08.0.80
Technology / Technology Group	Stacking - Traditional Stacking

Issue	FI-194945
Symptom	When an ICX device's TCAM is exhausted with IP Source Guard (IPSG) entries, if another host comes in the ICX device will get into a state where the IPSG entry for the new host is not written to the TCAM but the entry is remembered in the persistent storage. If the ICX device reloads in this state, when the system comes up none of the IPSG entries restored from the persistent storage will be programmed in the tcam and even the default deny rule will not get programmed. This means any host will get permitted from that point onwards.
Condition	This problem happens only when the ICX device's learnt entries in the IPSG software table exceeds the available TCAM space on the ICX device "and" the ICX device reloads in that situation.
Workaround	Learnt IPSG entries within the TCAM capacity will not result into the issue. No hardware errors will be seen and eventual problem during reload won't happen. When TCAM failure errors are seen while learning an IPSG client, release the client entry so that there will not be any stale entries in software tables. This will avoid running into this issue.
Recovery	
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Security - IP Source Guard

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 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	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.
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

Issue	FI-192258
Symptom	Device will be detached from stack and the device will come up as standalone unit.Issue is seen on ICX-7850_48FS product
Condition	Issue is seen with higher IPSG scale entries around ~1500 per stack unit, and when stack unit comes up after stack reload.
Workaround	There is no workaround.
Recovery	Operator need to remove dhcp configuration and also clear DHCP snooping entries, save this updated configuration and then trigger reload of device.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Security - IP Source Guard

Issue	FI-188576
Symptom	On an ICX7850, Egress ACL applied on Virtual interface (VE) will not be honored as per the user configuration if an only if untagged ports part of the Vlan.
Condition	1. On ICX 7850 platform, Configure Vlan with untagged ports. 2. Configure VE for corresponding VLAN and apply egress ACL bindings to VE interface.
Workaround	No Workaround
Recovery	None
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-191748
Symptom	On ICX7850 switch/Router, when we have multiple protocols enabled (like LACP, MACSEC) and we are learning scale number of ip source guard entries (approximately 1500),we may see CPU spike and protocols flap.
Condition	On ICX7850 switch/Router, enable LACP and MACSEC, and try to learn beyond 800 ip source guard entries. The High CPU will not occur if the number of IPSG entries learnt are less than 800 in the system
Workaround	No workaround.
Recovery	
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Security - IP Source Guard

Issue	FI-190860
Symptom	On an ICX7850, when a large is ACL configured/unconfigured on default VLAN with multiple ports, CPU spike around 40 - 50% seen approx for 1 min. While protocol flaps are not seen with the number of protocol sessions that were present, it is possible that there could be protocol flaps when we scale the sessions.
Condition	The issue happens when the following conditions are met 1. per-port-per-valn enabled 2. IPv4 and IPv6 ingress ACL configured with >=800 filters in each of these ACLs 3. system default VLAN has >= 40 ports
Workaround	To bind a large ACL, create an ACL with small number of filters (<= 50) and bind it first, followed by adding the rest of the filters one by one to the ACL. To unbind a large ACL, remove filters one by one and once the number of filters is small (<= 50), the ACL can be unbound
Recovery	The system will come back to normal state by itself after that 1min cpu spike
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-188432
Symptom	An ICX 7K stack does not do PBRv6 based forwarding for packets in the slow path. These packets would get forwarded based on the regular L3 forwarding tables in the slow path
Condition	This was observed when TCP MSS was enabled on an interface of the ICX stack. This can happen to any slow path packets for which are supposed to be PBRv6 forwarded.
Workaround	No workaround
Recovery	No Recovery
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-195181
Symptom	few syslog messages "acl_hitless_sg_acl_update: ACL ptr not found" are seen on Standby Unit's session after reload.
Condition	if ip source guard is enabled on the ports belonging to stanby unit, these messages will be seen on the console.
Workaround	no loss of functionality, kindly Ignore these messages.
Recovery	No recovery
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Security - IP Source Guard

Issue	FI-183744
Symptom	Link flaps for standby unit ports of the LAG(s) when a large ACL is applied
Condition	It happens when the following two conditions are met 1. UDLD is enabled on the link (of the LAG) which is on the Standby Unit 2. The ACL has more than 1000 filters
Workaround	To bind a large ACL, create an ACL with small number of filters (<= 50) and bind it first, followed by adding the rest of the filters one by one to the ACL. To unbind a large ACL, remove filters one by one and once the number of filters is small (<= 50), the ACL can be unbound
Recovery	The system will recover automatically and come back to normal state
Probability	
Found In	FI 08.0.80
Technology / Technology Group	

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