

FastIron 09.0.00 for Ruckus ICX Switches Release Notes Version 1

Supporting FastIron 09.0.00

Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

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, COMMSCOPE 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. CommScope 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. CommScope 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 CommScope 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 COMMSCOPE, COMMSCOPE 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 COMMSCOPE 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, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Document History	5
Introduction	7
About RUCKUS FastIron Release 09.0.00.....	7
Document Feedback.....	7
RUCKUS Product Documentation Resources.....	8
Online Training Resources.....	8
Contacting RUCKUS Customer Services and Support.....	8
What Support Do I Need?.....	8
Open a Case.....	8
Self-Service Resources.....	9
New in This Release	11
Hardware	11
Software Features.....	11
New Software Features in 09.0.00.....	11
Important Changes in Release 09.0.00.....	12
CLI Commands.....	13
New Commands for FastIron 09.0.00.....	13
Modified Commands for FastIron 09.0.00.....	14
Deprecated Commands for FastIron 09.0.00.....	16
RFCs and Standards.....	20
MIBs	20
Hardware Support	21
Supported Devices	21
Default Username and Password.....	21
Supported Power Supplies.....	21
Supported Optics.....	21
Upgrade Information	23
Image File Names.....	23
PoE Firmware Files.....	23
Open Source and Third Party Code.....	24
Known Issues in Release 09.0.00	27
Resolved Issues in Release 09.0.00	41

Document History

Version	Summary of changes	Publication date
FastIron 09.0.00 for ICX Switches Version 1	<ul style="list-style-type: none">• New software features and enhancements• Introduction of the ICX7850-48C platform• The ICX 7750 is no longer supported• Known and Resolved issues	July 27, 2021

Introduction

- [About RUCKUS FastIron Release 09.0.00](#)..... 7
- [Document Feedback](#)..... 7
- [RUCKUS Product Documentation Resources](#)..... 8
- [Online Training Resources](#)..... 8
- [Contacting RUCKUS Customer Services and Support](#)..... 8

About RUCKUS FastIron Release 09.0.00

RUCKUS FastIron release 09.0.00 introduces the RUCKUS ICX7850-48C switch, the newest member to the ICX 7850 series. This switch delivers premium performance and scalability for Data Center Top-of-Rack/Leaf deployments requiring 10GbE RJ-45 connectivity with 100GbE uplink to the Spine/Aggregation layer. This switch is also ideal for 10GbE workstation aggregation design and engineering development workgroup clusters.

Release 09.0.00 also introduces several new features and manageability enhancements including the following:

- New, simplified Web UI with a new management architecture, firmware upgrade capability, and configuration backup and restore.
- RESTCONF support, which provides a programmatic interface into ICX
- DHCP client scale support is increased from 500 to 3000 clients
- Configuration archive and replace functionality through CLI
- Introduction of the Flexlink feature for detecting link failures
- Multicast enhancements for improved Video over Ethernet deployments.

Refer to the [Software Features](#) on page 11 section of this document for a complete list of features and enhancements in release 09.0.00.

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@commscope.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

Introduction

RUCKUS Product Documentation Resources

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 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 11
- Software Features..... 11
- Important Changes in Release 09.0.00..... 12
- CLI Commands..... 13
- RFCs and Standards..... 20
- MIBs 20

Hardware

FastIron Release 9.0.00 introduces the RUCKUS ICX7850-48C Switch.

The ICX7850-48C supports the following features:

- 48x1G/10G RJ45 (10GBASE-T) ports
- 8x 40/100 GbE QSFP28 ports supporting native 40 GbE or 100 GbE, or breakout to 4x10 GbE or 4x25 GbE (breakout not support with stacking)
- 8x100G QSFP28 ports for uplink/stacking
- PHY-less design for QSFP28 ports
- 2x hot-swappable load sharing power supplies and 5x hot-swappable fan assemblies with reversible airflow options (Power supplies and FAN airflows must be the same)

Software Features

The following section lists new, modified, and deprecated software features in release 09.0.00.

New Software Features in 09.0.00

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	Description
ACLs on CPU Ports	Brings in the ability to control traffic destined for CPU. Examples include ICMP packets, DHCP packets etc., User will be able to apply access-lists to allow/drop CPU-bound packets matching the ACL rules
Breakout support on the ICX 7550	A 40-Gbps breakout cable can be used on ICX 7550 standalone units to convert some 40-Gbps ports into four 10-Gbps subports. Alternatively, a 100/40 Gbps cable can be used in an ICX 7550 standalone switch to break-out certain 40-Gbps ports into four 10-Gbps subports and 100 Gbps ports into four 25-Gbps subports, respectively.
Copy UFI image and manifest from flash to USB	ICX switches and routers will have the ability to copy a UFI image and manifest file from flash to USB using the CLI.
Configuration Archive and Replace	ICX switches and routers have the flexibility to back-up and store multiple configuration files in flash. These backed up files can be copied to running configuration to manage system configuration when needed.
DHCPv4 client scale	IP DHCP binding scalability has been enhanced to support up to 3000 clients.

New in This Release

Important Changes in Release 09.0.00

Feature	Description
100-Gbps stacking support on the ICX 7550	100-Gbps stacking support has been included in ICX 7550
IPv6 Source Guard	FI 09.0.0 introduces IPv6 Source Guard support which can be used with IPv6 Neighbor Discovery Inspection (NDI) on untrusted ports.
RESTCONF	RESTCONF is an IETF standard to configure network devices programmatically. It is a successor to REST API and NETCONF configuration protocols and is primarily driven by YANG models that describe the network configurations and operations. RESTCONF can now be used to programmatically configure ICX devices.
Multicast enhancements for Software Defined Video-over-Ethernet (SDVoE)	Software Defined Video-over-Ethernet (SDVoE) is a software-based AV-over-IP platform that provides solutions for point-to-point connectivity and Ethernet-based audio visual (AV) distribution. A number of enhancements have been introduced for SDVoE.
New web UI	FI 09.0.00 introduces a brand-new web user interface with monitoring, configuration, remote CLI, and firmware upgrade capabilities.
Web authentication white-lists	Users can now allow Web Authentication clients to access more than one website or server during the authentication process. The white-list can be defined using IPv4 addresses or FQDN entries.
Energy Efficient Ethernet (EEE) on ICX 7550 Copper Ports	EEE regulates and saves power consumed by the active hardware components in the switch and conserves power during idle time.
Flexlink	Flexlink is a link redundancy feature that provides Layer 2 resilience. It is an alternative solution to Spanning Tree Protocol (STP) as it provides link redundancy at a faster network convergence rate than STP and its variants RSTP/ MSTP.
IP Based MLD Snooping	IP based MLD snooping is a functional enhancement that ensures multicast forwarding entries use Group Address, Source Address, and VLAN as key from this release onwards. This change can now start supporting source-specific multicast deployment scenarios.
VXLAN on the ICX 7550	VXLAN support is extended to the ICX 7550 devices.
PTP support on ICX 7550 and ICX 7650	PTP support is extended to ICX7550-24F, ICX7550-48F, ICX7650-48F, and ICX7650-48ZP devices.

Important Changes in Release 09.0.00

The following changes were introduced in FastIron Release 09.0.00:

- Campus Fabric is not supported in FastIron 09.0.00 or later releases. Campus Fabric is supported in 08.0.95 and will continue to be supported in 08.0.95 maintenance releases.
- Release 09.0.00 and future releases do not support ICX 7750 devices. The ICX 7750 is supported in 08.0.95 and will continue to be supported in 08.0.95 maintenance releases.
- Release 09.0.00 does not support ICX-Management from SmartZone or ICX-Management from the Cloud. SmartZone management (SZ 6.1) support will be added in FastIron release 09.0.10.
- Remote Network Monitoring (RMON) is not supported in 09.0.00.
- Beginning in 09.0.00, ICX 7150 and ICX 7250 platforms are limited to a maximum of eight units in a stack.
- Image copy using the system-manifest will accept only "/". The system will not accept "\" as it did in 08.0.95 and earlier releases.
- HTTPS is enabled by default.
- All access to ICX devices is via username and password only. Login without a username or without a password is no longer supported.
- To access LAG interface configuration, you must enter the LAG interface number. You can no longer access LAG interface configuration using the member ports.

- Beginning with 09.0.00 release, the logs that are generated using the debug and distributed logger utilities are sent to the Log Manager. The Log Manager infrastructure provides the capability to store the application log files in a centralized repository. The centralized repository can be accessed to display the log files using the **show logging debug** command. Log manager is enhanced to upload the fetched logs to an external server. It also allows you to monitor real-time updates to the specified logs on local units.
- The following authentication methods are no longer supported:
 - line (enable via Telnet password)
 - enable (via configured password for Super-User level privileges)
 - TACACS
- Release 09.0.00 introduces changes to ICX digital certificate commands and parameters, including the following:
 - Only TFTP or SCP can be used for importing certificates.
 - HTTPS is enabled by default and no longer has to be configured for SSL server configuration.
 - Only RSA keys can be used.
 - Available maximum key sizes are 4096 (the default) and 2048 bits.
 - Some SSL certificate CLI commands have changed.
 - Users are no longer allowed to generate self-signed certificates on ICX switches

Refer to the [Software Features](#) on page 11 section for a list of new features 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.

CLI Commands

The commands listed in this section were introduced, modified, or deprecated in FastIron 09.0.00.

New Commands for FastIron 09.0.00

The following commands have been added (new for this release).

- **cfg-archive management archive-size**
- **cfg-archive management compare-archives**
- **cfg-archive management compare-running-config**
- **cfg-archive management copy**
- **cfg-archive management copy-running-config**
- **cfg-archive management delete**
- **cfg-archive management list**
- **cfg-archive management reload-with-archive**
- **cfg-archive management rename**
- **cfg-archive management show-archive-content**
- **clear dlogger logs**
- **cli timeout**
- **dlogger redirect**
- **dlogger module**
- **flexlink backup**
- **flexlink preemption delay**
- **flexlink preemption mode**

New in This Release

CLI Commands

- interface cpu active
- ip multicast edge-port
- ip multicast flood-unregistered
- ip multicast static-mcache profile
- ipv6 multicast flood-unregistered
- logmgr fetch
- logmgr help
- logmgr hierarchy
- logmgr monitor
- logmgr upload
- management access
- management source-interface
- management vrf
- restconf enable
- restconf config-sync
- restconf config-sync-interval
- restconf enable-config-sync
- restconf platform-debug-level
- restconf protocol-debug-level
- show dlogger logs
- show dlogger module
- show flexlink
- show ip multicast static-mcache-profile
- show ip multicast vlan
- show ip ssl device-certificate
- show log debug management restconf all
- show restconf config
- show restconf event-counters
- show restconf status
- show restconf running-config
- show management access
- snmp-server log-suppress-timer
- white-list (Web Authentication)

Modified Commands for FastIron 09.0.00

The following commands have been modified (updated for this release).

- aaa authentication enable
- aaa authentication login
- aaa authentication snmp-server

- **aaa authentication web-server**
- **banner**
- **copy disk0 flash**
- **copy flash disk0**
- **copy tftp flash**
- **crypto key client generate**
- **crypto key client zeroize**
- **crypto key generate**
- **forwarding-profile**
- **hmon client configuration**
- **hmon client statistics**
- **hmon client status**
- **hmon status**
- **interface ve**
- **ip dhcp-client ve**
- **ip ssh authentication-retries**
- **ip ssh idle-time**
- **ip ssl min-version**
- **multi-stack-port**
- **multi-stack-trunk**
- **multicast fast-leave-v2**
- **multicast sdvoe**
- **multicast static-mcache profile**
- **option**
- **rconsole**
- **show arp**
- **show ethernet loopback interfaces**
- **show ip dhcp-client options**
- **show ip multicast mcache**
- **show ip ssh**
- **show ip ssh sessions**
- **show ip ssl**
- **show ipv6 multicast mac-mcache**
- **show ipv6 multicast mcache**
- **show ipv6 multicast optimization**
- **show mac access-lists**
- **show manager counters**
- **show manager status**
- **show memory**

New in This Release

CLI Commands

- `show running-config vlan`
- `show snmp`
- `show tech-support`
- `show web`
- `show webauth`
- `snmp-server disable`
- `snmp-server enable traps`
- `stack-port`
- `stack-trunk`
- `supportsave`
- `username`
- `web-management`

Deprecated Commands for FastIron 09.0.00

The following commands have been deprecated in this release.

- `aaa authentication enable implicit-user`
- `aaa authentication login privilege-mode`
- `batch buffer`
- `clear ip dhcp-server statistics`
- `console timeout`
- `crypto-ssl certificate`
- `deploy`
- `enable aaa console`
- `enable cloud-only-password`
- `enable password-display`
- `enable strict-password-enforcement`
- `enable super-user password`
- `enable telnet authentication`
- `enable telnet password`
- `enable user password-masking`
- `exit-address-family`
- `exit-vrf`
- `flash`
- `inline power interface-mode-2pair-pse`
- `ip dhcp-client lease`
- `ip dhcp-server relay-agent-echo enable`
- `ip http client connection timeout connect`
- `ip multicast disable-flooding`
- `ip preserve-acl-user-input-format`

- **ip radius source-interface**
- **ip ssh permit-empty-passwd**
- **ip ssh pub-key-file**
- **ip ssh strict-management-vrf**
- **ip ssh source-interface**
- **ip ssl cert-key-size**
- **ip ssl certificate**
- **ip ssl certificate-data-file tftp**
- **ip ssl client-certificate tftp**
- **ip ssl client-private-key tftp**
- **ip ssl port**
- **ip ssl private-key-file tftp**
- **ip syslog source-interface**
- **ip tacacs source-interface**
- **ip telnet source-interface**
- **ip tftp source-interface**
- **ipv6 multicast disable-flooding**
- **management-vrf**
- **manager source-interface**
- **max-vlan (SPX)**
- **max-vlans-per-pe-port**
- **module (SPX)**
- **multi-spx-lag**
- **multi-spx-port**
- **pe-id**
- **pe-name**
- **radius-server enable vlan**
- **rconsole (SPX)**
- **router-interface**
- **scp (license)**
- **service password-encryption**
- **show arp inspect**
- **show configuration (SPX)**
- **show dot1x configuration**
- **show dot1x ip-acl**
- **show dot1x mac-filter**
- **show dot1x sessions**
- **show dot1x sessions detail**
- **show dot1x statistics**

New in This Release

CLI Commands

- **show ip dhcp-server statistics**
- **show ip ssh rekey statistics**
- **show ip ssh tcp-forwarding**
- **show ip ssl**
- **show ip ssl client-certificate**
- **show ip ssl profile**
- **show ip static-arp**
- **show ip tcp status**
- **show mac access-lists name**
- **show mac-authentication configuration**
- **show mac authentication ip-acl**
- **show mac-authentication sessions**
- **show mac-authentication sessions detail**
- **show mac-authentication statistics**
- **show file-manger config**
- **show file-manager logs**
- **show management traffic exclusion**
- **show spx**
- **show spx cb-port**
- **show spx connections**
- **show spx csp**
- **show spx debug**
- **show spx lag**
- **show spx mecid**
- **show spx multicast cache**
- **show spx multicast counters**
- **show spx multicast optimization**
- **show spx multicast resource**
- **show spx pe-id**
- **show spx pe-group**
- **show spx pe-port-vlan-resources**
- **show spx ring**
- **show spx zero-touch ipc**
- **show spx zero-touch log**
- **show spx zero-touch status**
- **show spx-mon**
- **show stack link-sync**
- **show startup-config (SPX)**
- **show transmit-counter**

- **snmp-client**
- **snmp-server enable mib**
- **snmp-server max-ifindex-per-module**
- **snmp-server trap-source**
- **source-interface (ntp)**
- **spx allow-pe-movement**
- **spx cb-configure**
- **spx cb-enable**
- **spx interactive-setup**
- **spx pe-enable**
- **spx ping**
- **spx suggested-id**
- **spx unconfigure**
- **spx unit**
- **spx zero-touch-deny**
- **spx-lag**
- **spx-mon enable**
- **spx-port**
- **ssh access-group**
- **system-max session-limit**
- **system-max view**
- **tacacs-server enable vlan**
- **telnet access-group**
- **telnet client**
- **telnet login-retries**
- **telnet login-timeout**
- **telnet server suppress-reject-message**
- **telnet timeout**
- **terminal logging**
- **tftp client enable vlan**
- **tftp server ip-address image-location**
- **verify**
- **web access-group**
- **web client**
- **web-management allow-no-password**
- **zero-touch-enable**
- **zero-touch-ports**

RFCs and Standards

There are no newly supported RFCs or standards in release 09.0.00.

MIBs

The following MIBs were introduced or updated in 09.0.00:

- DHCPv6 Snoop MIB
- FlexAuth MIB
- NDI MIB

Hardware Support

- Supported Devices 21
- Supported Power Supplies..... 21
- Supported Optics..... 21

Supported Devices

The following devices are supported in release 09.0.00.

- ICX 7150 Series (ICX 7150-C08P, ICX7150-C08PT, ICX7150-C10ZP, ICX7150-C12P, ICX7150-24, ICX7150-24F, ICX7150-24P, ICX7150-48, ICX7150-48P, ICX7150-48PF, ICX7150-48ZP)
- ICX 7250 Series (ICX7250-24, ICX7250-24G, ICX7250-24P, ICX7250-48, ICX7250-48P)
- ICX 7450 Series (ICX7450-24, ICX7450-24P, ICX7450-48, ICX7450-48F, ICX7450-48P)
- ICX 7550 Series (ICX7550-24, ICX7550-48, ICX7550-24P, ICX7550-48P, ICX7550-24ZP, ICX7550-48ZP, ICX7550-24F, ICX7550-48F)
- ICX 7650 Series (ICX7650-48P, ICX7650-48ZP, ICX7650-48F)
- ICX 7850 Series (ICX7850-32Q, ICX7850-48FS, ICX7850-48F, ICX7850-48C)

Default Username and Password

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 Web. 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.

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 <https://www.commscope.com/globalassets/digizuite/61722-ds-ethernet-optics-family.pdf>.

NOTE

Optics and transceivers are being re-branded from Brocade to RUCKUS, which includes changes to labels and serial numbers.

Upgrade Information

- [Image File Names.....](#) 23
- [PoE Firmware Files.....](#) 23
- [Open Source and Third Party Code.....](#) 24

Image File Names

Download the following FastIron 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.

For detailed instructions on how to upgrade to a new FastIron release, see the [RUCKUS FastIron Software Upgrade Guide](#).

Device	UFI file name (boot, image)
ICX 7150	SPR09000ufi.bin/SPS09000ufi.bin
ICX 7250	SPR09000ufi.bin/SPS09000ufi.bin
ICX 7450	SPR09000ufi.bin/SPS09000ufi.bin
ICX 7550	GZR09000ufi.bin/GZS09000ufi.bin
ICX 7650	TNR09000ufi.bin/TNS09000ufi.bin
ICX 7850	TNR09000ufi.bin

PoE Firmware Files

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

Device	Firmware version	File name
ICX 7150	2.1.8 fw	icx7xxx_poe_02.1.8.b004.fw
ICX 7250	2.1.8 fw	icx7xxx_poe_02.1.8.b004.fw
ICX 7450	2.1.8 fw	icx7xxx_poe_02.1.8.b004.fw
ICX 7550	1.54.0 fw	icx7xxx_poe_01.54.00.b001.fw
ICX 7650	2.1.8 fw	icx7xxx_poe_02.1.8.b004.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.

Upgrade Information

Open Source and Third Party Code

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/xcouple-datalink** in Privileged EXEC mode or in interface configuration mode using the command **inline powercouple-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.
- 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.

Third Party Software	Open source (Yes/No)
avl	Yes
Aquantia - PHY Drivers	No
Broadcom - SDK	No
Broadcom - PHY Drivers	No
Broadcom - Linux	Yes
Broadcom - Uboot	Yes
Broadcom/Marvell - sysroot	Yes
ZeroMQ - Library for Inter Process Communication	Yes
Trusted Computing Group - TPM	Yes
libunwind	Yes
Source for rootfs (Part of Linux)	Yes
Dynamic (.so) and static(.a) libraries	Yes
iptables	Yes
python3	Yes
Ingy dot Net - YAML Parser, libyaml-0.2.5	Yes
diffios - conf_archive	Yes
IP Infusion - MVRP	No
WindRiver - IPSec	No
WindRiver - PKI	No
WindRiver - OSPFv3	No
OpenSSL	Yes
Bind9	Yes

Third Party Software	Open source (Yes/No)
Network Security Services (NSS)	Yes
WindRiver - SNMP	No
curl	Yes
zlib	Yes
libxml	Yes
python	Yes
Nginx - szagent Uwsgi - szagent curl - szagent zlib - szagent libxml - szagent	Yes
flask_package - webui node_module - webui openssl - webui	Yes
OpenSSH - SSH client / server	Yes
Python-PAM - Python based PAM authentication module	Yes
Pyrad - Radius	Yes
Tacacs_plus - Tacacs+	Yes
Linux-Pam - PAM authentication	Yes
Radsecproxy - Proxy radius server	Yes
Nettle - Cryptographic library for radsecproxy	Yes
ISC - DHCPv6 Server	Yes
ISC - DHCPv4 server client	
Abduco - Console	Yes
FCGI2 - RESTConf	Yes
FCGIWrap - RESTConf	Yes
Nginx - RESTConf/Web	Yes
Libtelnet - RConsole	Yes
Busybox - Telnet	Yes
Ulogd - Management access	Yes
SSL - OpenSSL	Yes

Known Issues in Release 09.0.00

This section lists open software issues with Critical, High, and Medium Technical Severity in FastIron 09.0.00.

Issue	FI-244642
Symptom	Default user password update does not reflect for restconf authentication
Condition	If startup config does not have any users configured or on erase startup configuration and reload, we will be forced to change the default super/sp-admin login.
Workaround	Create a privileged user if not present. Delete and readd default super user with new password for restconf to authenticate with new super user credentials
Recovery	Create a privileged user if not present. Delete and readd default super user with new password for restconf to authenticate with new super user credentials
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-242838
Symptom	In Show tech output some command captures are displayed multiple times
Condition	Execution of 'Show tech' CLI command
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-235801
Symptom	In switch mode, ICX management VLAN outband interface might broken after system reloading
Condition	management VLAN ACL rule TCAM programming error caused the issue. Recommend management VLAN configure no more than one member port; if need multiple ports, bind the ports into an LAG.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.90
Technology / Technology Group	Management - IPv4/IPv6 Host Management

Known Issues in Release 09.0.00

Issue	FI-241728
Symptom	syslog timestamp is not in sync with system clock.
Condition	When a timezone other than GMT is configured, syslog timestamp will not be in sync with "show clock" CLI output
Workaround	None
Recovery	configure system timezone as "GMT+00" using the CLI "clock timezone gmt gmt+00"
Probability	
Found In	FI 09.0.00
Technology / Technology Group	Management - NTP - Network Time Protocol

Issue	FI-241498
Symptom	After stack failover or switchover, Vxlan will not be operational, if previous Vxlan unconfigure operation hadn't happened in a particular order.
Condition	Execute no lag(access & tunnel) followed by no overlay gateway.
Workaround	Unconfigure overlay before deleting lag
Recovery	None.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-241070
Symptom	Ipv6 load sharing of traffic stops after disabling and enabling the ecmp link.
Condition	Disable ecmp link and load-sharing, again re-enable ecmp link and load-sharing
Workaround	When the issue is seen, following steps can be done for work around 1. Disable the missing ecmp link 2. Re-enable the ecmp link. Doing above 2 steps will fix the issue.
Recovery	
Probability	
Found In	FI 09.0.00 FI 10.0.00
Technology / Technology Group	

Issue	FI-240966
Symptom	DHCP Client connected to switch configured with dhcp-gateway list are not assigned dynamic ip address
Condition	DHCP Client connected to switch configured with dhcp-gateway list are not assigned dynamic ip address
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-240035
Symptom	"debug cluster" commands are not supported in 9.0. These CLIs are used by TAC/developers to debug MCT issues. However, now these commands are not used to debug issues anymore.
Condition	The commands under "debug cluster" will not be available on 9.0 image.
Workaround	The below commands are available to debug MCT. dm l2-debug mdup-ctrl dm l2-debug cluster-ctrl fitrace modules cluster_mct
Recovery	None.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-239865
Symptom	If the Banner MOTD is configured, it will be displayed after the Telnet, SSH, or Console session is successfully authenticated similar to any Linux system.
Condition	banner motd needs to be configured
Workaround	No workaround available
Recovery	No recovery available
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-239843
Symptom	Console session freezes when applying scaled configuration by pasting it directly on the console
Condition	Apply scaled configuration in console using copy paste
Workaround	Use SSH or telnet session for applying scaled configuration
Recovery	Reapply the missed configs.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-226915
Symptom	Inter-vlan routing or ping to directly connected hosts not working with deny ACL, when permit PBR is enabled
Condition	deny ACL and permit PBR configuration via CLI
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Security - PBR - Policy-Based Routing

Known Issues in Release 09.0.00

Issue	FI-223864
Symptom	Ping from any host to customer CPE device(IP received via dhcp) routed via ICX router was not working.
Condition	Change the mode of customer CPE device from Router Mode to Bridge Mode
Workaround	
Recovery	Delete the static route configured wait for sometime and reapply of static route helps in recovery Reboot of ICX device also helps
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

Issue	FI-220756
Symptom	CPU spike every 5min when ICX has 50+VLAN and managed by SZ
Condition	1. Configure 50+ Vlans in the ICX 2. Connect the device with SZ. 3. High CPU consumption will be observed
Workaround	Remove the empty and unused VLANs.
Recovery	None
Probability	
Found In	FI 08.0.90 FI 08.0.92 FI 08.0.95
Technology / Technology Group	

Issue	FI-238921
Symptom	Running a CLI command 'logmgr fetch all all all', displays unwanted message. There is no loss in functionality.
Condition	Running the CLI command 'logmgr fetch all all all' displays unwanted message on the console. Applies to stacks only.
Workaround	None, just a display issue.
Recovery	None, just a display issue.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-238422
Symptom	When multiple line banner message is configured from SZ, all the lines in the message doesn't get configured due to the input string not being in expected format and error message doesn't get displayed for the same.
Condition	when multiple line banner message is configured from SZ using cli templates and if each line is not terminated with ^C character
Workaround	
Recovery	when configuring from SZ, terminate each line in the banner string with ^C character, similar to how its displayed in the show running
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-238309
Symptom	For webauth client trying to access URL with extensions like path after the domain name, www.google.com/Images/xyz, then browser is not getting redirected to webauth login page. When the client/user types only domain names like ww.google.com then http client will be redirected to webauth login page
Condition	Client tries to access URL with path extensions like http://www.yahoo.com/file/xyz.jpg
Workaround	
Recovery	
Probability	High
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-238200
Symptom	HTTPS is always enabled by default in 9.0 and supports all SSL protocols TLSv1/TLSv1.1/TLSv1.2. The commands to create self signed certificate have been deprecated in 9.0, the config shall not be applied and not present in running configuration after upgrade. The self signed cert created shall be migrated and always present until the user overwrites it with new cert/key which can be done using copy cmds.
Condition	Upgrading from previous releases where users had self-signed certificates generated on ICX.
Workaround	No impact as the previous certificate will be retained until a new certificate is copied.
Recovery	Not applicable
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-238003
Symptom	In ICX 7650, 10G Fiber port LEDs may not blink in stat mode with traffic sometimes
Condition	In ICX 7650, 10G Fiber port LEDs may not blink in stat mode with traffic sometimes
Workaround	no workaround
Recovery	no recovery
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-237965
Symptom	With RADIUS server accounting enabled on device, on verification of accounting logs in RADIUS server.The RADIUS accounting logs shows invalid internal IP address in NAS-IP-Address.
Condition	This symptom is seen only when management source-interface for RADIUS is configured with non-default VRF
Workaround	Management source-interface for RADIUS can be configured in default VRF
Recovery	Not available
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Known Issues in Release 09.0.00

Issue	FI-237820
Symptom	If ACL in PBR route-map has "log" configured, then traffic match with PBR rule will not only be forwarded based on PBR route-map, but also be trapped to CPU and be forwarded out by CPU. So two copy of ingress traffic will be forwarded out.
Condition	
Workaround	Please remove "log" from ACL configuration if such ACL is used by PBR route-map.
Recovery	Please remove "log" from ACL configuration if such ACL is used by PBR route-map.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-237720
Symptom	ICX Switch/Router crashes during ISSU upgrade.
Condition	Run ISSU command on ICX Switch/Router.
Workaround	No Workaround
Recovery	No Recovery
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-237530
Symptom	No error message displayed when an outbound SSH connection fails to get established
Condition	The outbound "ssh" connection error message will not be displayed in the CLI.
Workaround	NA
Recovery	NA
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-237237
Symptom	Memory usage increased from 67% to 88% during upgrade from FI 8.0.95 to 9.0.00 on ICX 7150 stack.
Condition	Upgrade ICX 7150 from FI 8.0.95 to 9.0.00
Workaround	
Recovery	
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-236807
Symptom	The Configuration from CLI doesn't reflected in the RESTCONF running-config
Condition	If customer has RESTConf feature enabled and retrieves the RESTConf config through CLI command and not from RESTConf Management Interface
Workaround	Retrieve the RESTConf GET from RESTConf Management Interface and not from CLI command.
Recovery	
Probability	Medium
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-236356
Symptom	when doing image update from uboot, 7850 devices might show an error "Synchronous Abort" handler" and gets rebooted
Condition	when doing image update from uboot, 7850 devices might show an error "Synchronous Abort" handler" and gets rebooted
Workaround	No workaround available
Recovery	system automatically reloads from the error for recovery, user needs to retry the operation.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-236181
Symptom	The show running configuration will always show correct output. But some of the mac addresses for 'show auth acl all' will not display output when used with filters. SSH@ICX7450-48-Router#show authentication acls all i "0022.9696.03f0"
Condition	User executes show CLI command with ' ' filter and uses long filters
Workaround	use filter with lesser characters or execute without filter search option SSH@ICX7450-48-Router#show authentication acls all i 03f0 1/2/2 0022.9696.03f0 - - - -
Recovery	
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-236104
Symptom	On rare occasions, PoE Auto firmware upgrade could fail
Condition	On rare occasions, PoE Auto firmware upgrade could fail
Workaround	None
Recovery	A reboot can help in retrying PoE auto upgrade to recover.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Known Issues in Release 09.0.00

Issue	FI-235501
Symptom	In command line interface, on usage of '?' character for help throws unexpected value "st[2][H[H" ICX7850-48FS Router(config)#router bgp Enable bgp msdp Enable msdp ospf Enable ospf pim Enable pim rip Enable rip vrrp Enable vrrp vrrp-extended Enable vrrp-extended vsrp Enable vsrp ICX7850-48FS Router(config)#router st[2][H
Condition	Using '?' in automation scripts with console
Workaround	Skip additional character after the prompt, use SSH or TELNET
Recovery	Carriage return to go to next line
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-232698
Symptom	Following commands will not be available to the user. batch NSlookup show log debug management plugin all
Condition	
Workaround	NSlookup - All FQDN resolution to IP/IPv6 addresses will happen using DNS. CLI command will not be available for this release show log debug management plugin all - the component logs can be collected using supportsave
Recovery	
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-232632
Symptom	Privilege command is not available in command line interface.
Condition	When user logs in to ICX device using SSH/TELNET/CONSOLE, privilege command is not seen either in help or when executed. These commands will be removed from the configuration when upgrading from previous releases to 09.0.0 release.
Workaround	User can configure privilege in external RADIUS/TACACS+ server and login using RADIUS/TACACS + user. For local user workaround is not available for privilege.
Recovery	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-232445
Symptom	The below snmp-server commands will not be available snmp-server community <string> ro rw <acl_name acl_id> snmp-server community <string> ro rw ipv6 <acl_name> snmp-server group <string> v1 v2c v3{auth noauth priv} access <acl_id> ... snmp-server group <string> v1 v2c v3{auth noauth priv} access ipv6 <acl_name> ... snmp-server user <user> <group_name> v3 access <acl_id> ...
Condition	When user tries to configure above mentioned commands from CLI.
Workaround	Not Applicable
Recovery	Not Applicable
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-232145
Symptom	"Timeout" Error will be seen, while doing SNMP set of object "snAgGblPassword".
Condition	SNMP set of Object snAgGblPassword
Workaround	Not Applicable
Recovery	Not Applicable
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-230954
Symptom	on configuring authentication methods as radius followed local or local followed by radius, if user authentication fails with first auth-method, 2nd auth-method is not getting triggered.
Condition	auth-methods in webauth must be radius followed by local (or) local followed by radius.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-230401
Symptom	When system-max vlan is configured as 3 and rebooted, it misses configuring of tagged ports on user vlans and invalid lag interface being added to default vlan.
Condition	This issue is observed when user tries to configure <5 vlans as system-max.
Workaround	The user should configure at least 5+ vlans as maximum vlans in system-max.
Recovery	Configure system-max as 5+ vlans and reload the system.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Known Issues in Release 09.0.00

Issue	FI-225997
Symptom	In ICX7150, optic might show as empty even when it is present
Condition	In ICX7150, optic might show as empty after multiple and frequent plugin and plugout of optics
Workaround	Any optic plugout or plugin should be done gently
Recovery	Plugout and plugin the optic gently.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-224766
Symptom	10G SFP plugged into ICX7850 can cause the port to flap twice before the link comes up
Condition	When a 10G SFP plugged into ICX7850, the port may flap twice before the link comes up
Workaround	no workaround
Recovery	no recovery needed, system works normally after the flap
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-222417
Symptom	L3 unicast forwarding not working
Condition	1.stack-switchover 2.reload of new active unit
Workaround	None
Recovery	None
Probability	Low
Found In	FI 09.0.00
Technology / Technology Group	Layer 3 Routing/Network Layer

Issue	FI-220109
Symptom	no interface ethernet <port> sometimes does not clear the configuration under the interface
Condition	When "ipv6-neighbor inspection trust" configuration is preset, no interface ethernet <port> does not clear the configuration under the interface
Workaround	remove the mentioned configuration individually before trying 'no interface ethernet" command
Recovery	remove the mentioned configuration individually before trying 'no interface ethernet" command
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-213575
Symptom	On ICX7150, the ARP resolution happens on an openflow-hybrid L23 Interface.
Condition	Issue is specific to Openflow on ICX7150
Workaround	Sending Tagged traffic OR having a MAC Table entry will prevent flooding.
Recovery	Changing the interface type to a non-hybrid interface thereby preventing the un-tagged packets from being redirected to the L2/L3 Processing by default will stop the traffic from flooding.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-193316
Symptom	The configured rate-limit will be changed when mld or igmp rate-limit (any one) is disabled once after the rate-limit configuration is set for mld and igmp.
Condition	1. On ICX device configure both IGMP and MLD snooping on two different VLANs. 2. Configure multicast ratelimit. 3. Disable IGMP Snooping or MLD Snooping (any one) under both the VLANs. The effective rate-limit for multicast packets will be changed which is unexpected.
Workaround	No Workaround.
Recovery	No Recovery.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Layer 2 - Link Aggregation

Issue	FI-209506
Symptom	The IPv4 route table full SYSLOG message will be generated though the hardware table is not full.
Condition	With more VRFs configured, if the advertised BGP routes to all the VRFs are increased more than MAX route per VRF, sometimes the hardware route table is not added with MAX route per VRF and route table full SYSLOG will be thrown.
Workaround	Disabling and Enabling the interface will add back the routes upto MAX route per VRF.
Recovery	
Probability	Low
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - Multi-VRF

Known Issues in Release 09.0.00

Issue	FI-210895
Symptom	Few IPv6 routes will fail in installation to HW in the scenarios mentioned in the condition for this to occur.
Condition	Few IPv6 routes will fail in forwarding profile 1 (default profile) in following particular sequence of execution o Two BGP neighbors - V4 & V6 o First establish V4 neighbor and send 300K /24 routes o After the HW table in full sync, establish V6 neighbor and send 11K /64 routes o Then bring down V6 neighbor and on V4 send 300K Custom prefix routes (without affecting the session) o Then establish V6 neighbor and send 11K V6 Custom prefix routes. o At this point we are seeing few hundreds of routes are failed to add to HW
Workaround	Clear both v4 and v6 routes
Recovery	Clear both v4 and v6 routes
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-214157
Symptom	BUM(Broadcast-Unknown unicast-Multicast) traffic coming from VxLAN network port leaks to VxLAN access port which is in BLOCKED state.
Condition	Physical loop in VxLAN access ports side topology and spanning tree(Any flavor of spanning tree) is configured on VxLAN access ports to break the loop.
Workaround	None except avoiding loop on VxLAN access port side.
Recovery	None.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-217519
Symptom	When a mvrp enabled lag interface is deleted, then recreate the same lag interface again (when lag has member ports from standby unit as well), there are some errors thrown. Then it does not allow to configure mvrp under lag interface.
Condition	This issue is observed when lag has member ports from standby and active both.
Workaround	Workaround - This issue can be avoided If mvrp enabled lag port is disabled first .Then this issue of lag delete and recreate operation with MVRP is not seen.
Recovery	lag interface and mvrp functionality can be restored back by adding back the lag interface to mvrp untagged vlan.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-216126
Symptom	High CPU on ICX Routers/Switches with User ACL scale with logging enabled and high data traffic
Condition	Configure scaled Ipv4, IPv6 and MAC ACLs on ICX devices with logging enabled. High data traffic matching the ACLs will result in high CPU.
Workaround	Disable logging feature with high data rate.
Recovery	No recovery.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Resolved Issues in Release 09.0.00

This section lists software issues with Critical, High, and Medium Technical Severity that were resolved with a code change in release 09.0.00.

Issue	FI-239069
Symptom	port microflaps on connecting to ICX7150-stack retimer ports (1/3/4 or 2/3/4)
Condition	Configure retimer port as 1g and use 1G SX SFP for connection
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	System - System

Issue	FI-240156
Symptom	Sometimes ICX might experience unexpected reload during vSZ registering
Condition	vSZ HTTP service unavailable response 503 error might cause unexpected reload of ICX device.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.95
Technology / Technology Group	Management - Management GUI

Issue	FI-238999
Symptom	ICX running config SZ backup operation failure
Condition	When management VRF is configured, ICX UDP port forwarding was failed, which may cause ICX running config backup failure. Management VRF UDP port forwarding support has been added to fix the problem
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.90
Technology / Technology Group	Management - Management GUI

Issue	FI-224274
Symptom	ICX switch running switch image duplicate unicast ARP Request packets causing multiple ARP replies for a single request
Condition	1. Send ARP Request packet not destined to the switch.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.92
Technology / Technology Group	

Resolved Issues in Release 09.0.00

Issue	FI-227599
Symptom	When ICX unit joins the stack, it will get into reboot loop
Condition	1. "system-max ip-route" is configured on ICX. 2. An ICX unit is joining the stack
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-231100
Symptom	10G link stays down after multiple reboots(70 to 400) of peer device(FXT)
Condition	Unplug and replug 10G OPTIC/SFP on ICX7850 and Reboot peer device(FXT) multiple times
Workaround	None
Recovery	One of the below steps helps in recovery 1)Reload of peer FXT device 2)Reload of ICX 3)disable and enable the port on ICX(sometimes it is not working)
Probability	Low
Found In	FI 08.0.90
Technology / Technology Group	System - System

Issue	FI-236979
Symptom	Manually configured hostname is not saved when dynamic host name is set.
Condition	1. DHCP Option 12 hostname and switch hostname is also configured with the same name. 2. When DHCP release happens, Switch hostname is reverted to default hostname
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.92 FI 08.0.95
Technology / Technology Group	Management - Configuration Fundamentals

Issue	FI-235053
Symptom	Unexpected reload of the device might be experienced in ICX 7650 and ICX 7850.
Condition	Unexpected reload of the device can happen when processing incoming packet.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Management

Issue	FI-238497
Symptom	QSFP read errors might be thrown while dumping EEPROM contents on switch for 40GE-Active Copper 5m (QSFP+) link
Condition	While dumping EEPROM contents on switch for 40GE-Active Copper 5m (QSFP+) link, QSFP read errors might be thrown
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.90
Technology / Technology Group	System - Optics

Issue	FI-239022
Symptom	Traffic stopped passing through MCT
Condition	upgrade from 8095 to 9.0
Workaround	None
Recovery	no deploy and deploy on both peers helped in recovery
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Layer 2 Switching - MCT - Multi-Chassis Trunking

Issue	FI-226377
Symptom	In a stack setup when active unit goes down EBGp route entries are not deleted properly and cause routing issue.
Condition	When active stack unit is powered off, some IP routes are not properly deleted from routing table. The new active unit does not delete BGP learned routes with nexthop only reachable from the previous active unit.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.90
Technology / Technology Group	Layer 3 Routing/Network Layer - BGP4 - IPv4 Border Gateway Protocol

Issue	FI-236657
Symptom	Removing ICMP/TCP burst cause ping to loopback ip to fail
Condition	TCP/ICMP burst config is removed, ping to loopback IP will fail
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	Layer 3

Resolved Issues in Release 09.0.00

Issue	FI-233347
Symptom	TFTP transfer failing from Cisco router (used as tftp server) to ICX due to no TFTP rollover feature
Condition	Lack of TFTP rollover feature causing tftp transfer to fail .
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Other - Other

Issue	FI-231381
Symptom	Outbound SSH session from ICX will fail when the SSH server password start with "!"
Condition	1. SSH server password start with "!" 2. Establish Outbound SSH session for the server from ICX
Workaround	NA
Recovery	NA
Probability	Low
Found In	FI 08.0.90
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-229372
Symptom	Mitel phones not getting the phone server IP address.
Condition	When ICX is used as DHCP Server, Mitel phones not getting the phone server IP address through DHCP option 43.
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.90 FI 08.0.92 FI 08.0.95
Technology / Technology Group	Management - DHCP (IPv4)

Issue	FI-225203
Symptom	ICX port might be stuck in down state after peer Cisco device port flap
Condition	1. Port Down/Up peer Cisco Device 2. ICX Port stuck in Down state.
Workaround	Flap ICX peer end port
Recovery	
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-226756
Symptom	10G link stays down after multiple reboots(3 to 18) of peer device(FXT)
Condition	Unplug and replug 10G OPTIC/SFP on ICX7850 and Reboot peer device(FXT) multiple times
Workaround	None
Recovery	One of the below steps helps in recovery 1)Reload of peer FXT device 2)Reload of ICX 3)disable and enable the port on ICX(sometimes it is not working)
Probability	Low
Found In	FI 08.0.90
Technology / Technology Group	System - System

Issue	FI-238511
Symptom	When short path forwarding is enabled under VRRP-E, ARP entry to VIP is not learned or points to invalid port. So traffic fails.
Condition	Happens always if short-path forwarding is enabled on VRRP-E backup router.
Workaround	1. Configuring static arp entry mapping VIP to VMAC resolves the issue. 2. Removing short path forwarding also resolves the issue.
Recovery	1. ARP entry with VRRP-E MAC will be learned if short-path forwarding is disabled in VRRP-E backup router. 2. Configuring static arp entry mapping VIP to VMAC resolves the issue
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - VRRPv2 - Virtual Router Redundancy Protocol Version 2

Issue	FI-237237
Symptom	Memory usage increased from 67% to 88% during upgrade from FI 8.0.95 to 9.0.00 on ICX 7150 stack.
Condition	Upgrade ICX 7150 from FI 8.0.95 to 9.0.00
Workaround	
Recovery	
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-236622
Symptom	In ICX7150, L3 traffic is not passed through module 3.
Condition	When stacking is disabled and the stack ports 1/3/1 and 1/3/3 are used as data ports, L3 traffic is not passed through
Workaround	
Recovery	
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - IP Addressing

Resolved Issues in Release 09.0.00

Issue	FI-234257
Symptom	The link between ICX-7850-48FS and ICX-7550-48ZP is up on ICX7550 side and down on ICX7850 side.
Condition	When connected with 1Gb fiber SFP, the link between ICX-7850-48FS and ICX-7550-48ZP is up on ICX7550 side and down on ICX7850 side
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	System - Optics

Issue	FI-232127
Symptom	Fortinet FAP-431F Access Point is not getting powered on switch reboot.
Condition	If inline power power-limit is set, then AP(Fortinet FAP-431F) is not getting powered on switch reboot.
Workaround	Issue is not seen with 1) default inline power config 2) inline power power-by-class 3.
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	Management - PoE/PoE+ - Power over Ethernet

Issue	FI-218769
Symptom	ICX7550 with 1G Fiber port with 100-fx connected optic may not link up
Condition	ICX7550 with 1G Fiber port with 100-fx connected optic may not link up
Workaround	None. 100-fx optic is not supported in ICX7550 in 9.0 release
Recovery	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-236268
Symptom	In ICX7150, L3 traffic is not passed through module 3.
Condition	When stacking is disabled and the stack ports 1/3/1 and 1/3/3 are used as data ports, L3 traffic is not passed through.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-234574
Symptom	IPv6 subnet 127 point-to-point interface address configuration might be wrongly treated as duplicated address.
Condition	IPv6 subnet 127 point-to-point interface address configuration.
Workaround	NA
Recovery	Do disable and enable interface could recover sometimes.
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Other

Issue	FI-229352
Symptom	SSH login being rejected
Condition	In very rare case, the deleted SSH sessions were not fully cleaned up causing the SSH sessions resource not re-usable, thus new SSH login was out of resource and rejected.
Workaround	work around: 1. do crypto key zeroize "Router(config)# crypto key zeroize" 2. regenerate crypto key "Router(config)# crypto key generate"
Recovery	None
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-234759
Symptom	"inline power detail" command might show the PoE Firmware version as 0.0 occasionally
Condition	continuous running of "inline power detail" command might show the PoE Firmware version as 0.0 occasionally
Workaround	no workaround
Recovery	no recovery needed. Automatically recovers on the next instance of the command
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-234043
Symptom	on rare conditions, ICX7850 could continuously crash during bootup
Condition	on rare conditions, ICX7850 could continuously crash during bootup
Workaround	None
Recovery	clear the configuration from uboot
Probability	
Found In	FI 09.0.00
Technology / Technology Group	Other - Other

Resolved Issues in Release 09.0.00

Issue	FI-227217
Symptom	Switch is using none VE 1 IP addressed to join the Ruckus Cloud
Condition	if a user has a (none) VE 1 configure with the IP Address, Switch will use the none VE 1 IP address to join the cloud. If the switch goes to factory reset and try to join the cloud.
Workaround	Remove the None VE 1 configuration from the UI before joining the Ruckus Cloud
Recovery	Remove the None VE 1 configuration from the UI before joining the Ruckus Cloud
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-228332
Symptom	The routes learnt through BGP are not deleted from routing table for 10 min after the peer is down.
Condition	When the Standby unit in the Stack is powered off, through which EBGp routes are learnt, some of the IP routes are not deleted for 10 min after the peer is down.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.90 FI 08.0.92 FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - BGP4 - IPv4 Border Gateway Protocol

Issue	FI-225709
Symptom	OSPF routes are not seen in the Areas in which they are not originated.
Condition	After reload, OSPF routes not seen in the Areas in which they are not originated.
Workaround	Disabling and Enabling the interface through which the routes are originated.
Recovery	
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Layer 3 Routing/Network Layer - OSPF - IPv4 Open Shortest Path First

Issue	FI-179229
Symptom	Radius Authentication Configuration lost after reboot if the radius key is longer than 45 characters. "Error: RADIUS key can have maximum of 64 characters" during boot up.
Condition	1. Radius key configuration with key size more than 45 characters followed by reload. 2. Tacacs+ key configuration with key size more than 45 characters followed by reload. 3. Radius coa client key configuration with key size more than 45 characters followed by reload.
Workaround	NA
Recovery	NA
Probability	Medium
Found In	
Technology / Technology Group	Security - RADIUS

Issue	FI-219985
Symptom	In some ICX7150-48PF and ICX7150-48P devices port 1/3/4 doesn't come up.
Condition	The issue is seen if both stacking ports (1/3/1, 1/3/3) are up and running then port 1/3/4 doesn't come up.
Workaround	The workaround is to use linear topology and configure the 2nd stack port as 1G.
Recovery	None
Probability	
Found In	FI 08.0.90 FI 08.0.92
Technology / Technology Group	System - Optics

Issue	FI-218957
Symptom	While booting ICX7550 may show the message "ERROR: PLL Lock Failed" in the console and fail to boot from the preferred boot partition
Condition	on multiple reloads, ICX7550 may not boot from the preferred boot partition
Workaround	Maintain stable images on other partition, so that system boot with other partition. Then copy image to the partition where observed ERROR.
Recovery	reload the system from the correct partition
Probability	
Found In	FI 09.0.00
Technology / Technology Group	Other - Other

Issue	FI-217913
Symptom	7150 stuck in boot mode after power outage
Condition	Power outage
Workaround	None
Recovery	TFTP of FI image needs to be done from boot prompt at primary or secondary
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	System - System

Issue	FI-218550
Symptom	7150 stuck in boot mode after power outage
Condition	Power outage
Workaround	None
Recovery	update 8095 firmware from uboot using tftp and then update 9.0 firmware
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	System - System

Resolved Issues in Release 09.0.00

Issue	FI-219089
Symptom	Incorrect watch port was displayed while retrieving open flow dump-groups information from the controller.
Condition	1. Configure open-flow groups in the ICX using open flow controller. 2. Retrieve open flow dump-groups information using controller.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.80 FI 08.0.92
Technology / Technology Group	

Issue	FI-222686
Symptom	Unexpected value is displayed for actual speed in "show interface lag x" command output
Condition	When one of the stack member unit is down, "show interface lag x" command displays wrong speed.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.92
Technology / Technology Group	System - CLI

Issue	FI-223444
Symptom	No PoE functionality on one or more member units of stack. PDs on member unit ports are not powered.
Condition	When a stack is rebooted or upgraded, some of the units might not initialize PoE functionality.
Workaround	reload the unit where PoE is not functional using "reload unit <unit-id>". Or upgrade to latest image.
Recovery	reload the unit where PoE is not functional using "reload unit <unit-id>".
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-221538
Symptom	Unable to stack the units with stack zero touch or manually.
Condition	Unable to stack the units with stack zero touch or manually when the Stack ports 1/3/x and 1/4/x are 10G.
Workaround	
Recovery	Stacking is allowed with the ports 1/3/x and 1/4/x only if 40G ports.
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Stacking - Stack Management

Issue	FI-220743
Symptom	Not able to remove/change auth-def-vlan configuration from an interface
Condition	Configure Auth-default-vlan configuration in Multi Interface configuration Mode
Workaround	Best option is to change global Auth-def-vlan if it involves multiple ports and only change under interface for few of them, in which case, individual ports can be changed
Recovery	
Probability	Low
Found In	FI 08.0.90
Technology / Technology Group	Security - MAC Port-based Authentication

Issue	FI-217958
Symptom	Port continues being part of MSTP after doing no spanning-tree on the interface
Condition	Tried to remove port from MSTP
Workaround	None
Recovery	do spanning-tree and no spanning-tree on interface for recovery
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Layer 2 Switching - xSTP - Spanning Tree Protocols

Issue	FI-220431
Symptom	MACsec link of ICX7450 might fail to be established after a reboot of one of the peers
Condition	MACsec is not supported on all four ports of module 2 (4x10G) if stacking is enabled and the default stacking ports are 1/2/1 and 1/2/3.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Security - MACsec - Media Access Control security

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	

Resolved Issues in Release 09.0.00

Issue	FI-215630
Symptom	Stacking ports utilization might suddenly go high
Condition	Stack port utilization might go high without any trigger
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Stacking - Traditional Stacking

Issue	FI-199756
Symptom	ICX7750 displays 8gig as the available memory but actual mem in use is only 4gig.
Condition	"show memory" command displays wrong memory size for ICX7750
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	System - CLI

Issue	FI-218550
Symptom	7150 stuck in boot mode after power outage
Condition	Power outage
Workaround	None
Recovery	update 8095 firmware from uboot using tftp and then update 9.0 firmware
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	System - System

Issue	FI-217597
Symptom	When ISSU command is used in a campus fabric setup, ISSU might abort and not complete.
Condition	The ISSU may abort when it is triggered on a campus fabric system, where port extender units have PoE capability.
Workaround	ISSU provides for an on-error option where the system can be reloaded from either primary or secondary partition when an ISSU abort is encountered. User can use this option to workaround this issue.
Recovery	The campus fabric system to be reloaded when the issue is encountered.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-218949
Symptom	In the console session, when logged in as super-user, the user may not be able to execute privilege level commands.
Condition	For the super user, when the privilege level is changed from super user to read-only mode.
Workaround	No workaround is available
Recovery	User has to exit from privileged EXEC mode to user EXEC mode and then re-enter to the privilege EXEC mode by entering the username and password.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-219133
Symptom	While SNMP walk query for wired client MIB OID returns wrong value
Condition	Query SNMP OID for IPv4 address in wired client MIB.
Workaround	No Workaround.
Recovery	No Recovery.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-202413
Symptom	ICX7650 / ICX7850 port connected to VDX will be down with port shut/no shut at VDX.
Condition	shut/no shut at VDX (or) port disable/enable at ICX.
Workaround	VDX port shut/no shut and ICX reload will recover the issue.
Recovery	NA
Probability	High
Found In	FI 08.0.70
Technology / Technology Group	System - Optics

Issue	FI-203682
Symptom	ISSU upgrade gets aborted in SPX setup.
Condition	When ISSU upgrade is done in SPX setup, occasionally PE unit is getting detached which causes the ISSU to be aborted.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Resolved Issues in Release 09.0.00

Issue	FI-216304
Symptom	When the ICX unit is reloaded, the system may trigger an unexpected coredump before the rebooting of the unit.
Condition	When the ICX unit is reloaded, the system may trigger an unexpected coredump before the rebooting of the unit.
Workaround	No workaround available.
Recovery	No recovery needed. System would automatically recover.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-208489
Symptom	Link may not come up when a 100M M-FX-SR SFP is used to connect to a remote device, after switch reboot.
Condition	Connect ICX and a remote device using 100M M-FX-SR SFP.
Workaround	NA
Recovery	Port disable and enable will recover the issue.
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	System - Optics

Issue	FI-217870
Symptom	40GE-LR4 links may not come up after reload.
Condition	After a power loss or a reload, some 40GE-LR4 links do not come up.
Workaround	Disable/Enable recovers the link.
Recovery	Another reload or disable/enable recovers the 40GE-LR4 link.
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	System - Optics

Issue	FI-218658
Symptom	ICX DHCP Client is not getting dynamic IP address.
Condition	When ICX DHCP Client is connected to Palo Alto DHCP Server, ICX is not getting the dynamic IP address assigned.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.92
Technology / Technology Group	Management - DHCP (IPv4)

Issue	FI-210309
Symptom	On Standalone ICX device which supports breakout ports (For Ex: 10x4g). DDoS Port Statistics OID for Breakout Ports will be skipped when the user initiates SNMP walk.
Condition	1. Configure DoS Protection on ICX device. 2. Initiate SNMP Walk for DDoS Port Statistics OID.
Workaround	User can fetch the DDoS port statistics using CLI command : "show statistics dos-attack"
Recovery	No Recovery Mechanism
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-202954
Symptom	DHCPv6 Snooping Table Doesn't have Entry for DHCPv6 Address
Condition	While IPv6 Addresses are getting allocated to hosts via DHCPv6 process and DHCPv6 Snoop is enabled on the Switch/Router, the snoop table have entry only for prefix but not for the Address
Workaround	No Work-Around
Recovery	No Recovery
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Security - IP Source Guard

Issue	FI-201580
Symptom	Mcast client sees traffic interruption when a new receiver connected to active unit joins the group or existing receiver connected to active unit leaves, other receivers connected to active unit experience a momentary traffic loss (few packets < 10).
Condition	Problem is seen when source is connected to standby and receivers are connected to active.
Workaround	Apply the command "no ip multicast-routing optimization oif-list all"
Recovery	Apply the command "no ip multicast-routing optimization oif-list all"
Probability	Medium
Found In	FI 08.0.80 FI 08.0.90 FI 08.0.91 FI 08.0.92 FI 08.0.95
Technology / Technology Group	IP Multicast - IGMP - Internet Group Management Protocol

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	
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

Resolved Issues in Release 09.0.00

Issue	FI-211410
Symptom	SNMP walk for DAI with IPaddress as index will show incorrect values.
Condition	1. Configure DAI on VLAN 2. SNMP walk on DAI MIB
Workaround	CLI show commands to fetch the DAI Dynamic and Static entries.
Recovery	No Recovery
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-211885
Symptom	When the MIRRORED port is on CB and Egress port MONITORING is on PE port then the known unicast packets are not getting forwarded.
Condition	When the CB port is configured as Mirrored port for Egress port monitoring of a port on PE and the unicast packets are not getting forwarded.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Monitoring - Port Mirroring

Issue	FI-213387
Symptom	IPv6 hardware route table full SYSLOG messages are generated when the hardware table is not full.
Condition	Only when there are more than 30K routes in a single VRF, these SYSLOG messages will be generated.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 - Other IPv6

Issue	FI-216418
Symptom	OSPFv3 sessions are in Loading state with uRPF and NSR configured along with triggers of multiple switchover
Condition	OSPFv3 sessions are in Loading state with around 2500 LSAs with NSR and uRPF configured with multiple stack switchovers for the OSPFv3 to go into loading state.
Workaround	Clearing the ospfv3 neighbor sessions bring the session back to full state
Recovery	Clearing the ospfv3 neighbor sessions
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-216753
Symptom	On ICX, After Addiing MAC ACL Ethertype via SNMP set operation. Removal of applied MAC ACL Ethertype filter via CLI configuration command will fail.
Condition	1. Configure MAC ACL Ethertype fitler OID via SNMP set. 2. Run "no" of the configured Ethertype filter via CLI configuration command.
Workaround	No Workaround.
Recovery	No Recovery.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-204617
Symptom	SNMP query for "snPortMacSecurityModuleStatTable" does not return all modules
Condition	Applies to ICX 7750
Workaround	
Recovery	
Probability	
Found In	FI 08.0.92
Technology / Technology Group	

Issue	FI-204270
Symptom	Few fields of the IGMP-STD-MIB (igmpInterfaceWrongVersionQueries, igmpCacheLastReporter) values on snmpget/snmpwalk will be undefined.
Condition	These fields are not supported by our software.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

