RELEASE NOTES

FastIron 09.0.10e for RUCKUS ICX Switches Release Notes Version 2

Supporting FastIron 09.0.10e

Part Number: 53-1005762-02
Publication Date: 20 February 2023

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, 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

Version	Summary of changes	Publication date
FastIron 09.0.10e for ICX Switch Version 1	• Including updates for FastIron Release 09.0.10a • ICX Management in the RUCKUS Cloud via HTTPs • Re-introduce strict password enforcement • Additional RESTCONF modules	February 10, 2023
FastIron 09.0.10e for ICX Switch Version 2	• Known and Resolved issues for FastIron 09.0.10e • Known issues for FastIron 09.0.10d	February 20, 2023

Overview

This release of Ruckus Cloud enables you to configure and manage Ruckus LTE APs and their services. WI-FI AP management is limited to evaluation/ demo level only using this version of Cloud release. Commercial WI-FI deployment, is only supported on Ruckus Cloud WI-FI release. Please contact your Ruckus representative for details.

About RUCKUS FastIron Release 09.0.10

NOTE

FastIron releases 09.0.00, 09.0.00a, and 09.0.10 are no longer available for download due to the discovery of a critical defect.

Refer to *TSB 2022-001 – FastIron 09.0.00 and 09.0.10 - Risk of Filesystem Corruption* on the Technical Support Bulletins page for more details.

RUCKUS recommends upgrading to FastIron release 09.0.10a or later for all ICX switches currently running any of the afore-mentioned releases.

All the software features supported in FastIron release 09.0.00, 09.0.00a, and 09.0.10 remain available and supported in FastIron release 09.0.10a and later releases unless specifically noted.

For completeness, the feature descriptions for all changes introduced in the unavailable releases; that is, FastIron 09.0.00, 09.0.00a, and 09.0.10, are included in this section.

RUCKUS FastIron release 09.0.10a 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.

FastIron release 09.0.10a introduces several new features and manageability enhancements. Key additions include the following:

- Support for MCT across ICX 7850 stacks as peers
- MACSec over VxLAN
- Web Authentication customization
- Multicast VLAN registration
- Packets/sec configuration for BUM traffic rate limiting
- 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, 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

NOTE
In-Service System Upgrade (ISSU) does not work for upgrade of FastIron release 09.0.10a or 09.0.10b, due to management changes in the 09.0.10b release.

Refer to Software Features on page 11 for a detailed list of features and enhancements in Fastron 09.0.10 releases.

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

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.commscope.com/ruckus .

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://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

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.commscope.com/ruckus 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://community.ruckuswireless.com
- 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

No new hardware was introduced in release 09.0.10.

Software Features

The following section lists new, modified, and deprecated software features in release 09.0.10 and subsequent patch releases.

New Software Features in 09.0.10e

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
ICX Management in the RUCKUS Cloud via HTTPs	This release adds support for HTTPs based ICX management in RUCKUS Cloud. Refer to the *RUCKUS FastIron Management Configuration Guide*
Strict Password Enforcement	Strict password enforcement, deprecated in FastIron 09.0.10a, is re-introduced in FastIron release 09.0.10e. With strict password enforcement, configured globally through the **enable strict-password-enforcement** command, new and modified passwords must be a minimum of 15 characters in length and must meet additional criteria as described in the *RUCKUS FastIron Security Configuration Guide*.
Additional RESTCONF modules	Added additional RESTCONF modules to the *RUCKUS FastIron RESTCONF Programmers Guide*.

New Software Features in 09.0.10d

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
Support for Network Segmentation	The release adds support for network segmentation using SmartZone 6.1.1.[1] The enhancement includes changes in Web authentication to accept a RADIUS-returned VLAN attribute for a Web authentication client, support for VxLAN remote site redundancy, and VNI scaling enhancements. Refer to the *RUCKUS FastIron Security Configuration Guide*.

Feature	Description
Dynamic Bootstrap Protocol (BOOTP) Support	BOOTP allows the DHCP server to assign an IP address or range of addresses to the BOOTP clients within its address pool. Refer to the *RUCKUS FastIron DHCP Configuration Guide*.
DHCP - IP to Physical Port Mapping	IP addresses can be reserved within a DHCP address pool against selected Ethernet ports. This allows any device connecting to the selected port on the switch to obtain the same IP address irrespective of the client identifier sent by the device. Refer to the *RUCKUS FastIron DHCP Configuration Guide*.
VXLAN with Routing in and out of tunnels (RIOT)	VXLAN with RIOT is supported from this release. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
VXLAN - VXLAN Network Identifier (VNI) Scale Enhancement	• A range of VLANs can be mapped to a VXLAN Network Identifier (VNI) for a VXLAN overlay-gateway. • A range of mapped VLANs can be extended over a VXLAN overlay-gateway. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
VXLAN Remote Site Monitoring and Redundancy	You can configure primary and secondary IP addresses for the remote endpoint of a VXLAN tunnel. In addition, you can configure a keep-alive timer and the number of retries to ensure that the tunnel is always established to an active endpoint. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
Proactive Monitoring of Cable Signal Errors and Logging	Proactive Monitoring of Cable Signal Errors and Logging helps to identify deteriorating cables in a network. Cable signal errors are identified proactively and, once errors are identified, a SYSLOG message is logged so that you can check and monitor the link. Refer to the *RUCKUS FastIron Monitoring Configuration Guide*.

New Software Features in 09.0.10c

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
MACsec data-delay protection	The MKA group configuration command **macsec delay-protection** has been added.
RMON	Remote Monitoring (RMON) support is restored beginning with this release.

New Software Features in 09.0.10b

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
MACsec Enhancements	Configurable MKA keychains applied at the interface level are introduced as an alternative to the individually configured pre-shared key. Refer to "Media Access Control Security" and "Creating and Configuring an MKA Keychain" in the *RUCKUS FastIron Security Configuration Guide*.

[1] SmartZone 6.1.1 is planned for release soon.

Feature	Description
RADIUS Security Enhancements	RADIUS server security (RADsec) is supported for Flexible authentication from this release. Previously, RADsec was supported only for Console login. **NOTE** On ICX 7250 and ICX 7450 series switches, the device trustpoint will not work with RADIUS due to the strict validation of certificates. For TLS with RADIUS on these switches, an external certificate needs to be copied to ICX in order to establish a successful TLS session. Refer to the *RUCKUS FastIron Security Configuration Guide*.
VXLAN Parameter Enhancements	Certain statistics pertaining to VXLAN virtual ports and VXLAN Network Identifiers (VNIs) can be collected and controlled. Additionally, you can clear statistics for an entire VXLAN gateway tunnel or for a particular VNI. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
ICX SSH Support for SHA-2 with 384 bits	An ICX device can be accessed using an ECDSA algorithm with 384-bit or 256-bit key sizes while connecting through SSH. Refer to the *RUCKUS FastIron Security Configuration Guide*.
SNMP Support for the RUCKUS VXLAN MIB	The VXLAN MIB lists the objects that give the management information for configuring the VXLAN feature. VXLAN MIB is a RUCKUS proprietary implementation. Refer to the *RUCKUS FastIron MIB Reference, 09.0.10b*.
SNMP Support for Fixed Rate-Limiting and Input Rate-Limiting	The Common Access Rate (CAR) MIB has been updated. Refer to the *RUCKUS FastIron MIB Reference, 09.0.10b*.
SNMP Support for FlexAuth Web Authentication Configuration	New OIDs are introduced to enable uplink ports in webauth configuration. Refer to the *RUCKUS FastIron MIB Reference, 09.0.10b*.

New Software Features in 09.0.10a

NOTE
FastIron releases 09.0.00, 09.0.00a, and 09.0.10 are no longer available for download due to the discovery of a critical defect.

Refer to *TSB 2022-001 – FastIron 09.0.00 and 09.0.10 - Risk of Filesystem Corruption* on the Technical Support Bulletins page for more details.

RUCKUS recommends upgrading to FastIron release 09.0.10a or later for all ICX switches currently running any of the afore-mentioned releases.

All the software features supported in FastIron release 09.0.00, 09.0.00a, and 09.0.10 remain available and supported in FastIron release 09.0.10a and later releases unless specifically noted.

For completeness, the feature descriptions for all changes introduced in the unavailable releases; that is, FastIron 09.0.00, 09.0.00a, and 09.0.10, are included in this section.

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
Layer 3 Priority Flow Control	Priority Flow Control has been extended to ICX 7850 devices at the global level. Refer to "Flow Control and Buffer Management" in the *RUCKUS FastIron QoS and Traffic Management Configuration Guide*.

Feature	Description
Configurable ICX SSH port for connection with SmartZone	The **manager ssh-port** command has been introduced to allow configuring a custom port for connecting to SmartZone. Refer to "Configuring a Custom Port Number for Connection to SmartZone" in the *RUCKUS FastIron Management Configuration Guide*.
MVR-Tagged VLAN Support	A number of changes and enhancements have been introduced for MVR. These include the following: • MVR is supported for both tagged and untagged receiver ports. • MVR is supported for router images only. • Query messages are supported for MVR. • Multicast data is supported for MVR. Refer to "Multicast VLAN Registration" in the *RUCKUS FastIron IP Multicast Configuration Guide*.
PTP Support on ICX 7150-48ZP	Precision Transparent Timing adds support for the ICX 7150-48ZP model. Refer to "Precision Time Protocol" in the *RUCKUS FastIron Management Configuration Guide*.
Supportsave Enhancements	Refer to "Supportsave" in the *RUCKUS FastIron Web Management Interface User Guide*.

DHCP Option 43 enhancement	In FastIron 09.0.00 and 09.0.10, DHCP Option 43, vendor-encapsulated-options, accepted only an ASCII string value.
	
	In FastIron release 09.0.10a, the **option** command is modified to accept hexadecimal values or IP addresses when specified. To accommodate this change, the syntax is modified as follows:
	
	option vendor-encapsulated-options { **ascii** *string* | **hex** *value* | **ip** *ip-address* }
	
	For example:
	
	`device# configure terminal`
	`device(config)# ip dhcp-server pool 1`
	`device(config-dhcp-1)# option vendor-encapsulated-options ip address 10.10.10`
	
	`device# configure terminal`
	`device(config)# ip dhcp-server pool 1`
	`device(config-dhcp-1)# option vendor-encapsulated-options hex 061731302e31302e31302e31302c31322e31322e31322e3132`
	
	`device# configure terminal`
	`device(config)# ip dhcp-server pool 1`
	`device(config-dhcp-1)# option vendor-encapsulated-options ascii test`
	
	Refer to the **option** command in the *RUCKUS FastIron Command Reference*.
	
	When the device is upgraded from FastIron 09.0.00 or FastIron 09.0.10 to FastIron 09.0.10a, the command modification is interpreted as follows:
	• The option followed by a valid hex value will add the value keyword **hex** and will interpret the following entry as a hex value.
	• The option followed by an IP address or a list of IP addresses will add the keyword **ip** and the entries as one or more IP addresses.
	• Any other value is considered an ASCII string, and the keyword **ascii** is added to the configuration.

One-Gbps Breakout Ports	Port density can be increased at the lower speed of 1 Gbps on a breakout port using this feature. You can change the speed of 10-Gps breakout ports to 1-Gbps breakout ports dynamically without performing a reload. Refer to the *RUCKUS FastIron Management Configuration Guide*.

Feature	Description
MCT-Stacking	ICX 7850 stacks can be configured as cluster peers in a Multi-Chassis Trunking (MCT) configuration. The LACP LAG capacity has been increased from 256 to 300 in this design. **NOTE** MCT support for ICX 7850 stacks as peers is of Beta quality in release 09.0.10 and is of production quality from the FastIron 09.0.10a patch. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
MCT Hitless Sequential Upgrade	MCT protocol version check is introduced to achieve MCT hitless upgrade. The new solution allows two units running 09.0.10 and higher software releases to form MCT peers, as long as their MCT protocol versions match and both peers are from the same model family. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
Multicast Routing PIM Enhancements over MCT	The following are supported on MCT clusters: • First-hop routing (FHR) and last-hop routing (LHR) • Anycast-RP • Rendezvous points (RPs) Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
MACsec over VXLAN	MACsec over VXLAN is an end-to-end security protocol that provides a secured environment to protect Ethernet frames traveling over IP networks. Although VXLAN provides Layer 2 extension across LAN/WAN, connections between sites are not secured. MACsec over VXLAN addresses this and achieves secured Layer-2 extension across LAN/WAN using cross-connect VNIs. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
TCP keychain	A configurable TCP authentication option (AO) keychain is supported. The settings can be applied to BGP and MSDP sessions. Refer to the *RUCKUS FastIron Security Configuration Guide* for information on configuring TCP keychain options. Refer to *RUCKUS FastIron IP Multicast Configuration Guide* to configure MSDP to use the keychain settings. Refer to *RUCKUS FastIron Layer 3 Routing Configuration Guide* to configure BGP to use the keychain settings.
New SSH key exchange method	The DH Group-14 SHA 256 key exchange method is supported for general use. Previously, this method was supported only in FIPS mode. Refer to the *RUCKUS FastIron Security Configuration Guide*.
Web management - AAA Settings	Configures the settings to enable web user authentication. Refer to the *RUCKUS FastIron Web Management Interface User Guide*.
Web authentication redirect page customization	Remove or modify UserID or Password labels on the authentication redirect page. Refer to the *RUCKUS FastIron Security Configuration Guide*.
Web authentication honoring the RADIUS-returned VLAN	Honor a RADIUS-returned VLAN for Web Authentication clients. Refer to the *RUCKUS FastIron Security Configuration Guide*.
Web Management - VLAN settings	Enhancements support the following: Clone VLAN Change Default VLAN Refer to the *RUCKUS FastIron Web Management Interface User Guide*.
Multicast VLAN Registration	Multicast VLAN Registration (MVR) enables more efficient distribution of multicast streams across Layer 2 networks, and the duplication of multicast streams from the same source is eliminated while maintaining isolation between hosts on different VLANs. Refer to the *RUCKUS FastIron Layer 3 Routing Configuration Guide*.

Feature	Description
Unknown Unicast Flood Block (UUFB)	UUFB blocks unknown unicast traffic on ports, including Link Aggregation Group (LAG) ports. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide*.
Packets-per-second log timer for BUM traffic rate limiting	Packets-per-second (pps) log timer and port dampening for pps ports are introduced. Refer to the *RUCKUS FastIron QoS and Traffic Management Configuration Guide*.
Disabling Multicast Static Group Forwarding for a VLAN	Multicast static group forwarding can be disabled at the VLAN Level. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
IGMP Filtering and State Limit	An IGMP report filter policy can be configured globally or for an Interface. Additionally, the maximum number of IGMP group addresses for the default VRF, or a non-default VRF instance, can be changed globally or at interface level. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
MLD Filtering and State Limit	An MLD report filter policy can be configured globally or for an interface. Additionally, the maximum number of MLD group addresses for the default VRF, or a non-default VRF instance, can be changed globally or at the interface level. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
IPv4 PIM Join Message Filter	IPv4 PIM devices can be configured to accept or reject Join and Prune messages for all the multicast group addresses and for all source addresses. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
IPv4 PIM Register Message Filter Rule	The register message filter rule for PIM can be configured so that unauthorized multicast sources or groups are blocked. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
IPv4 PIM Register Message Rate Limit	The maximum number of register packets sent or received per second by a device can be configured. The rate limit for the number of register messages can be set to a relatively low value to avoid adverse pressure on the CPU when numerous sources start concurrently. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
IPv6 PIM Join Message Filter	IPv6 PIM devices can be configured to accept or reject Join and Prune messages for all the multicast group addresses and for all source addresses. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
IPv6 PIM Register Message Filter Rule	The register message filter rule for IPv6 PIM can be configured so that unauthorized multicast sources or groups are blocked. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
IPv6 PIM Register Message Rate Limit	The maximum number of register packets sent or received per second by a device can be configured. The rate limit for the number of register messages can be set to a relatively low value to avoid adverse pressure on the CPU when numerous sources start concurrently. Refer to the *RUCKUS FastIron IP Multicast Configuration Guide*.
IPv4 Option Type Filters	Drop rules can be configured so that packets are dropped if certain condtions are not met. Refer to the *RUCKUS FastIron Layer 3 Routing Configuration Guide*.
IPv6 Extension Header Option Type Filters	Drop rules can be configured for IPv6 so that packets are dropped if certain condtions are not met. Refer to the *RUCKUS FastIron Layer 3 Routing Configuration Guide*.
Syslog threshold	Configure a threshold value to generate a warning message when log entries exceed the specified threshold. Refer to the *RUCKUS FastIron Monitoring Configuration Guide*.
System notification of PKI certificate expiration	The system sends notifications as certificates that cannot be renewed automatically are approaching expiration. Refer to the *RUCKUS FastIron Security Configuration Guide*.
Support Save	Support Save collects logs and information to help troubleshoot an issue. Refer to the *RUCKUS FastIron Monitoring Configuration Guide*.

Feature	Description
Secure Wipe	The Secure Wipe feature securely erases the flash contents permanently as per DoD 5220.22-M standards and reinstalls the FastIron device. Refer to the *RUCKUS FastIron Management Configuration Guide*.
Access authority to logging by privilege	The **username** command was modified so that a user privilege of 7 can be applied. A user with this privilege level cannot access the output of the **show logging** command.
Configuration archive auto-revert (commit and rollback)	The feature provides the capability to revert or rollback to a previous configuration if the changed running configuration is not saved to the non-volatile memory within a pre-defined time.
Logging buffer threshold and syslog alarm	The **threshold** option is added to the **logging buffered** command. When the threshold percentage is exceeded, the system generates a warning message.
WEB management enhancement	Added ability to manage and replace the configuration archive and ability to configure flow control.
Configuration archive max file capacity	The maximum configuration archive size has been expanded from 20 to 100 files.
DH Group-14 SHA 256 in non-FIPS mode	The DH Group-14 SHA 256 key exchange method is supported for general use.
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.
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.

Feature	Description
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.

Deprecated Software Features in 09.0.10a

The following software features are deprecated 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
RMON	The RMON protocol and commands are deprecated in FastIron release 09.0.10. RMON will be re-introduced in a subsequent patch release.

Important Changes in Release 09.0.10d

Per *Technical Support Bulletin TSB 2022-005 - Starting with release 8.0.95h/9.0.10d, products running a newer Power Over Ethernet (PoE) chipset do not support older releases*, the POE functionality in ICX 7150 and ICX 7450 devices that have the new MCU PD69220 will be turned off when connected in a stack running a pre-09.0.10d software image.

If you are installing an ICX 7150 or ICX 7450 device that contains MCU PD69220, you can prevent the POE capabilities of the device from being disabled by upgrading the stack to FastIron 09.0.10d or later firmware prior to installing the ICX 7150 or ICX 7450 device.

Refer to the Technical Support Bulletins page for more details.

Important Changes in Release 09.0.10a

NOTE
FastIron releases 09.0.00, 09.0.00a, and 09.0.10 are no longer available for download due to the discovery of a critical defect.

Refer to *TSB 2022-001 – FastIron 09.0.00 and 09.0.10 - Risk of Filesystem Corruption* on the Technical Support Bulletins page for more details.

RUCKUS recommends upgrading to FastIron release 09.0.10a or later for all ICX switches currently running any of the afore-mentioned releases.

All the software features supported in FastIron release 09.0.00, 09.0.00a, and 09.0.10 remain available and supported in FastIron release 09.0.10a and later releases unless specifically noted.

For completeness, the feature descriptions for all changes introduced in the unavailable releases; that is, FastIron 09.0.00, 09.0.00a, and 09.0.10, are included in this section.

The following changes were introduced in FastIron Release 09.0.10a:

- Campus Fabric is not supported in FastIron 09.0.10a or later releases. Campus Fabric is supported in 08.0.95 and will continue to be supported in 08.0.95 maintenance releases.
- Release 09.0.10a 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.
- Remote Network Monitoring (RMON) is not supported in 09.0.10a. It is re-introduced in 09.0.10c.
- Beginning in 09.0.10a, 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 suppported.
- 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 09.0.10a 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 confguration.
  - 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

  - All dynamic options, including the IP address, are relearned from the DHCP server once the ICX device reboots. All options are removed when the ICX device reboots, and are relearned when the ICX device comes back up.

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 09.0.10 and subsequent patch releases.

Re-Introduced Commands for FastIron 09.0.10e

The following commands have been re-introduced in this release.

- **enable strict-password-enforcement**

New Commands for FastIron 09.0.10e

No commands have been added in this release.

New Commands for FastIron 09.0.10d

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

- **dynamic-bootp**
- **extend vlan-range**
- **failure-detection (VXLAN)**
- **ip dhcp-server bootp ignore**
- **map vlan-range**
- **vxlan-riot**

New Commands for FastIron 09.0.10c

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

- **clear rmon statistics**
- **macsec delay-protection**
- **relative-utilization**
- **rmon alarm**
- **rmon event**
- **rmon history**
- **show relative-utilization**
- **show rmon alarm**
- **show rmon event**
- **show rmon history**
- **show rmon logs**

- **show rmon statistics**
- **system-max rmon-entries**

New Commands for FastIron 09.0.10b

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

- **authentication-algorithm (MKA)**
- **crypto openssl default-encoding**
- **keychain mka**
- **mka-keychain**
- **vni-counters**

New Commands for FastIron 09.0.10a

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

- **accept-register**
- **block unknown-unicast**
- **ccep-up-delay**
- **cfg-archive management archive-size**
- **cfg-archive management cancel-comparison**
- **cfg-archive management compare-archives**
- **cfg-archive management compare-running-config**
- **cfg-archive management compare-startup-config**
- **cfg-archive management copy**
- **cfg-archive management copy-running-config**
- **cfg-archive management delete**
- **cfg-archive management delete-unsaved-cfg**
- **cfg-archive management list**
- **cfg-archive management reload-with-archive**
- **cfg-archive management rename**
- **cfg-archive management show-archive-content**
- **cfg-archive management show-current-config**
- **cfg-archive management show-unsaved-cfg**
- **cfg-archive revert**
- **cfg-archive revert-option**
- **clear dlogger logs**
- **cli timeout**
- **dlogger redirect**
- **dlogger module**
- **flexlink backup**

- **flexlink preemption delay**
- **flexlink preemption mode**
- **icl-fwd-delay** (MCT)
- **interface cpu active**
- **ip dhcp snooping verify mac-address**
- **ip igmp access-group**
- **ip options drop**
- **ip multicast edge-port**
- **ip multicast flood-unregistered**
- **ip multicast mvr**
- **ip multicast static-mcache profile**
- **ip tftp blocksize**
- **ipv6 deny-undetermined-transport**
- **ipv6 drop routing-type**
- **ipv6 mld access-group**
- **ipv6 multicast flood-unregistered**
- **ipv6 options drop**
- **jp-policy**
- **keychain tcp**
- **logging enable tcp-ao**
- **logmgr fetch**
- **logmgr help**
- **logmgr hierarchy**
- **logmgr monitor**
- **logmgr upload**
- **management access**
- **management source-interface**
- **management vrf**
- **manager ssh-port**
- **multicast static-grp-fwd-disable**
- **multicast mvr**
- **rate-limit-pps-log**
- **register-rate-limit**
- **restconf enable**
- **restconf config-sync**
- **restconf config-sync-interval**
- **restconf enable-config-sync**
- **restconf platform-debug-level**
- **restconf protocol-debug-level**

- **securewipe**
- **show dlogger logs**
- **show dlogger module**
- **show flexlink**
- **show ip multicast mvr mvlan**
- **show ip multicast static-mcache-profile**
- **show ip multicast vlan**
- **show ip mvr interface**
- **show ip mvr mcache**
- **show ip mvr setting**
- **show ip pim jp-policy**
- **show ip ssl device-certificate**
- **show ipv6 pim jp-policy**
- **show log debug management restconf all**
- **show management access**
- **show restconf config**
- **show restconf event-counters**
- **show restconf status**
- **show restconf running-config**
- **show uufb enabled-ports**
- **snmp-server log-suppress-timer**
- **uplink-port** (Web Auth)
- **webpage custom-label**
- **webpage remove-user-id-label**
- **white-list (Web Authentication)**

Modified Commands for FastIron 09.0.10e

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

- management access
- show manager status

Modified Commands for FastIron 09.0.10d

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

- **cfg-archive revert-option**
- **show overlay-gateway**
- **show tech-support**
- **site (VXLAN)**
- **vrf forwarding**

Modified Commands for FastIron 09.0.10c

No commands have been modified in this release.

Modified Commands for FastIron 09.0.10b

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

- **clear overlay-gateway**
- **ip ssh key-exchange-method**
- **show dot1x-mka config**
- **show dot1x-mka sessions**
- **show keychain**
- **show overlay-gateway**

Modified Commands for FastIron 09.0.10a

The following commands have been modified in this release.

- **aaa authentication enable**
- **aaa authentication login**
- **aaa authentication snmp-server**
- **aaa authentication web-server**
- **banner**
- **broadcast limit**
- **cfg-archive management archive-size**
- **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 ssh key-exchange-method**
- **ip ssl min-version**

- **ip igmp max-group-address**
- **ipv6 mld max-group-address**
- **logging buffered**
- **map vlan to vni**
- **msdp-peer**
- **multi-stack-port**
- **multi-stack-trunk**
- **multicast fast-leave-v2**
- **multicast limit**
- **multicast sdvoe**
- **multicast static-mcache profile**
- **option**
- **option vendor-specific-options (option 43)**
- **priority-flow-control enable**
- **rconsole**
- **show arp**
- **show cluster**
- **show ethernet loopback interfaces**
- **show ip bgp neighbors**
- **show ip bgp vrf neighbors**
- **show ip dhcp-client options**
- **show ip igmp group**
- **show ip igmp interface**
- **show ip igmp settings**
- **show ip igmp traffic**
- **show ip msdp peer**
- **show ip multicast mcache**
- **show ip pim error**
- **show ip pim sparse**
- **show ip ssh**
- **show ip ssh sessions**
- **show ip ssl**
- **show ipv6 bgp neighbors**
- **show ipv6 mld settings**
- **show ipv6 mld traffic**
- **show ipv6 multicast mac-mcache**
- **show ipv6 multicast mcache**
- **show ipv6 multicast optimization**
- **show ipv6 pim error**

- **show ipv6 pim sparse**
- **show keychain**
- **show mac access-lists**
- **show manager counters**
- **show manager status**
- **show memory**
- **show running-config vlan**
- **show snmp**
- **show tech-support**
- **show web**
- **show webauth**
- **snmp-server disable**
- **snmp-server enable traps**
- **speed-duplex**
- **stack-port**
- **stack-trunk**
- **supportsave**
- **unknown-unicast limit**
- **username**
- **web-management**

Deprecated Commands for FastIron 09.0.10e

The following commands have been depcrecated in this release

- **ip dhcp-server arp-ping-timeout**

Deprecated Commands for FastIron 09.0.10d

No commands have been deprecated in this release.

Deprecated Commands for FastIron 09.0.10c

No commands have been deprecated in this release.

Deprecated Commands for FastIron 09.0.10b

No commands have been deprecated in this release.

Deprecated Commands for FastIron 09.0.10a

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**
- **clear web-connection**
- **console timeout**
- **crypto-ssl certificate**
- **deploy**
- **enable aaa console**
- **enable cloud-only-password**
- **enable password-display**
- **enable password-min-length**
- **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)**
- **rmon alarm**
- **rmon event**
- **rmon history**
- **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**
- **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 rmon**
- **show rmon statistics**
- **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 rmon-entries**
- **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 09.0.10.

MIBs

The following MIBs were introduced or updated in 09.0.10a:

- RFC 5643: MIB for Open Shortest Path First (OSPF) Version 3 (introduced)
- DHCPv6 Snoop MIB

- Flexible authentication MIB
- NDI MIB

The following MIBS were introduced or updated in 09.0.10b:

- VXLAN MIB
- Common Access Rate (CAR) MIB
- Flexible authentication MIB
- SNMP object snAgEraseConfig was added to erase start-up configuration from flash, and snAgSaveConfig was added to save running configuration to flash.

The following MIBS were introduced or updated in 09.0.10c:

- RFC 2819: RMON-MIB

The following MIBS were introduced or updated in 09.0.10d:

- VXLAN MIB

Hardware Support

Supported Devices

The following devices are supported in FastIron release 09.0.10a.

- 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

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.

NOTE
If a configuration migration is required between FastIron 09.0.10 and FastIron 09.0.10a or FastIron 09.0.10b, ISSU should not be used.

NOTE
In-Service System Upgrade (ISSU) does not work for upgrade of FastIron release 09.0.10a or 09.0.10b, due to management changes in the 09.0.10b release.

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	SPR09010eufi.bin/SPS09010eufi.bin
ICX 7250	SPR09010eufi.bin/SPS09010eufi.bin
ICX 7450	SPR09010eufi.bin/SPS09010eufi.bin
ICX 7550	GZR09010eufi.bin/GZS09010eufi.bin
ICX 7650	TNR09010eufi.bin/TNS09010eufi.bin
ICX 7850	TNR09010eufi.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 (PD69200) icx7xxx_poe_02.2.4.b002.fw (PD69220)
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 (PD69200) icx7xxx_poe_02.2.4.b002.fw (PD69220)
ICX 7550	1.54.0 fw	icx7xxx_poe_01.55.04.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.

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 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
Boradcom/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

Third Party Software	Open source (Yes/No)
OpenSSL	Yes
Bind9	Yes
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 ISC - DHCPv4 server client	Yes
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 Behavior

This section describes known behaviors for certain RUCKUS ICX devices and recommended workarounds where they exist.

New PD Disables PoE on ICX 7150 and ICX 7450 Devices in a Stack with Pre-09.0.10d Software

Per *Technical Support Bulletin TSB 2022-005 - Starting with release 8.0.95h/9.0.10d, products running a newer Power Over Ethernet (PoE) chipset do not support older releases*, the POE functionality in ICX 7150 and ICX 7450 devices that have the new MCU PD69220 will be turned off when connected in a stack running a pre-09.0.10d software image.

If you are installing an ICX 7150 or ICX 7450 device that contains MCU PD69220, you can prevent the POE capabilities of the device from being disabled by upgrading the stack to FastIron 09.0.10d or later firmware prior to installing the ICX 7150 or ICX 7450 device.

Refer to the Technical Support Bulletins page for more details.

ICX 7550 Port LED in PoE Mode

When a RUCKUS ICX7550-24ZP or a RUCKUS ICX 7550-48ZP device is operating in PoE mode and the user connects a PD to a 10-Gbps port, the port LED comes up green but immediately goes to amber, although the expected LED color is green.

When the PD is connected while the ICX device is not in PoE mode and is then placed in PoE mode, the port LED remains green as expected.

Workaround: If you encounter the issue, change the device to any other mode, or rotate to the PoE mode again. The LED will then work as expected.

Known Issues in Release 09.0.10e

Issue	FI-265296
Symptom	Snmp walk from "iso" fails in RMON-MIB::etherHistoryIntervalStart
Condition	SNMP Walk done from "iso" on a loaded system under stress
Workaround	Rerun the walk
Recovery	None
Probability	
Found In	FI 10.0.00
Technology / Technology Group	

Issue	FI-267916
Symptom	critical vlan can be removed, even if we configure auth-timeout-action as critical-vlan in flexauth configuration
Condition	configure auth-timeout-action critical-vlan and delete confgured critical-vlan
Workaround	we can remove critical vlan config using following steps in authentication mode 1.no auth-timeout-action critical-vlan 2. no critical-vlan
Recovery	No recovery needed
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-270056
Symptom	SNMPWALK after few hours prints "Timeout: No Response from xx.xx.xx.xx" and "Error in packet."Reason: (genError) A general failure occurred"
Condition	ISO MIB walk with scaled config
Workaround	Run snmpwalk from host machine with -d option enabled and -t as 30
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-270020
Symptom	1. An image copy is done to primary or secondary partition through any mode ?copy tftp/scp/ https ..? etc,. 2. User triggers system reload and system boots up with the partition where image is copied. 3. While system boots, it will start extracting the packages from the copied UFI image, a below message will appear during this time, Processing packages from primary partition Extract UFI FI version success, version = SPR09010e.bin New packages found, uninstalling old packages if any.. Installing packages, this may take some time 4. While on this message ?Installing packages, this may take some time?, all packages extraction will happen, in 7150 platform we see it takes around 5 minutes here. 5. During this time if system got some abrupt reboot, that is if ? powercycled?, powered OFF and then powered ON, currently system will go to OS> prompt on reboot after this powercycle here.
Condition	Device bootup will Not work if powercycled during firmware upgrade
Workaround	Same as in Recovery steps.
Recovery	1. In this case, system will go to OS> prompt and Manual recovery is needed. 2. In OS> prompt we need to execute 'reboot' command and then stop at uboot prompt by pressing "b". 3. If there is already any 8095 or old image in another partition, boot to that partition, or update another partition with 8095 or older release image. 4. Boot with that image, the system will bootup and console will be online. 5. Now recopy the new UFI image in both the partitions and reload the system, and it will get booted up fine and system will be upgraded now.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269995
Symptom	dm verify-cert failed with error
Condition	Using dm verify-cert CLI command
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-262794
Symptom	High CPU on ICX Switches may be observed when connected to Cloud.
Condition	High CPU may be observed when there is port flap or VLAN modification or xSTP Convergence
Workaround	None
Recovery	High CPU condition will be automatically recovered after 60-90min depending on the number of VLANs configured on switch.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269975
Symptom	issu is not working as expected after issuing the command "issu primary on-error reload-secondary"
Condition	Upgrade of Active unit failed
Workaround	Upgrade the software offline, using copy command
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269918
Symptom	OSPF configiuration of graceful-restart helper-disable is lost after upgrade.
Condition	OSPF configuration of graceful-restart helper-disable is lost.
Workaround	
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269886
Symptom	Multicast traffic loss observed in certain scenarios.
Condition	Rstp is enabled on the vlans in cluster and clients , but except for the vlan in which l3 mcast traffic is sent.
Workaround	Disable RSTP on Cluster vlans.
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Other - Other

Issue	FI-267411
Symptom	Flexauth blocked client's traffic is allowed instead of blocking.
Condition	Flexauth should configured on stack unit and have blocked users. if active unit gets un-conditional reload and gets elected as active again, then flexauth blocked clients traffic is allowed instead of restricting it.
Workaround	Unconfigure flexauth and re-configure flexauth.
Recovery	Recovery not applicable.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269805
Symptom	ACX UI is stuck in "Synchronizing data" status and below mentioned logs present with debug command. 1. show log debug management nats all "Failed to connect to 127.0.0.1 port 447: Connection refused" 2. show hmon client status all-clients The client status for Nginx is "Faulty".
Condition	NA
Workaround	NA
Recovery	Recover nginx by toggling below configuration. # config t # no web-management http
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269787
Symptom	System up time shows incorrect value, when ICX acts as SNMP host and ICX event details updated in SNMP Server.
Condition	1. Configure snmp-server host v2c /v3 on ICX box. 2. Add host detail in SNMP server. 3. Create a event on ICX like create vlan.
Workaround	
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269760
Symptom	when deleting snmp-server community by using "no snmp-server/snmp-server" command, device may go on a reload..
Condition	Deletion on snmp-server community string configuration
Workaround	none
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269681
Symptom	SNMP Walk on DHCP MIB may result in Telnet sessions getting disconnected and walk may timeout if a small timeout value is used.
Condition	In the DHCP Pool configuration, if no Excluded address range or Single Excluded address range or options configuration is there.
Workaround	Configure any dummy sub type configuration if possible. Increase the timeout value as necessary.
Recovery	NA
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269679
Symptom	Traffic is not forwarded based on source-route options in the packet.
Condition	Traffic is not forwarded based on source-route options in the packet.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269644
Symptom	Rx of LACP pkt is not happening on CCEP ports
Condition	This can happen when bm buffer allocated to lacp pkts is not freed
Workaround	
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269475
Symptom	SSH/Telnet fails
Condition	Reload in the active unit
Workaround	Nothing
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269463
Symptom	Management access rules for snmp-server community is not working as expected after configuring "no snmp-server" and "snmp-server"
Condition	configuring "no snmp-server", followed by "snmp-server" is not updating the rules linked to snmp-server community
Workaround	Reboot the device
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269275
Symptom	Unable to configure the boundary value of mentioned heartbeat value in "manager heartbeat-interval" configuration.
Condition	When below configuration is done: (config)#manager heartbeat-interval 5 Error: Wrong interval, Enter between 5 to 1800 seconds
Workaround	Use value between mentioned values.
Recovery	NA
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269249
Symptom	Configuration sync failed for module static syslog is seen during bootup.
Condition	This syslog is seen during reboot with no static route (configured/DHCP) configured. This doesn't have any functional impact.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269126
Symptom	Telnet / SSH login fails
Condition	NA
Workaround	Not available
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-268934
Symptom	Allow/ deny mgmt snmp-server rules doesn't apply as expected
Condition	When we configure rules for snmp-server user and group(which is associated to same user) with IPV4/ IPV6 ipaddress
Workaround	Configure different user and group for IPV6 and IPV4 address
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-268533
Symptom	After upgrade for 8.0.9x to 9.0.10db, group configuration with noauth option for ipv6 address is not present in running configuration.
Condition	IPv6 access entry for group configured with noauth option and upgrade from 8.0.9x to 9.0.10db
Workaround	Remove noauth option with SNMP server IPv6 before upgrade from 8.0.95
Recovery	Reconfigure the SNMP server group for ipv6 and associate with the management access entries. snmp-server group group12345 v3 noauth read all write all management access src-ipv6 <ipv6 add>/<prefix> allow/deny snmp-server group group12345 log
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-268513
Symptom	SNMP packet from a specific group is not denied , though deny configuration is applied for the specific group
Condition	When management access deny rule is configured for a specific group containing alphanumeric characters like group98765, the packet is not denied and snmpwalk is allowed for the specific group name. This scenario occurs after a reboot
Workaround	
Recovery	Remove the specific group configuration, and reconfigure with a different group name with the same deny configuration.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-268482
Symptom	If the stack unit priority is changed multiple times for standby and member units. Role change from member role to standby and vice versa is not happening.
Condition	Stack failover/role change is not happening after changing the stack unit priority
Workaround	Reload the member unit to recover the stack based on priority.
Recovery	Reload the units whose status appears as 'member if reloaded' / 'standby if reloaded'
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-268474
Symptom	Device taking longer time to bootup up with scaled management access configuration entries
Condition	"no snmp-server" configuration is present along with multiple management access entries(around 200)
Workaround	Restrict the number of management access configuration entries to 30
Recovery	NA
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-268366
Symptom	'snmp-server view' command not working in FI 09.0.10 or later
Condition	'snmp-server view' configured
Workaround	NA
Recovery	NA
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-268104
Symptom	Addition of a 9th unit to minion stack fails
Condition	Reload in the active unit is observed.
Workaround	NA
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-267958
Symptom	Monitor config is missing under vlan while do "copy tftp running"
Condition	When config file with monitor config is applied using "copy tftp running". due to depandant config and order of config command execution by config apply module.
Workaround	configure monitor config manually after "copy tftp running"
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-267840
Symptom	The ICX failover to standby cluster failed.
Condition	When standby cluster is a fresh install in Geo Redundancy services of SZ.
Workaround	NA
Recovery	When ICX cannot connect SZ , input command "manager disable" and "no manager disable" on ICX.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-267723
Symptom	Customer is observing that local users after login failures are still disabled even after the recovery time.
Condition	Issue observed after enabling "enable user disable-on-login-failure" command via configuration mode and local user has a number of login failures specified in the command.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-267687
Symptom	CPU is 99% when the traffic is on through standby unit port and DDOS is enabled.
Condition	This is an existing issue from day 1 specific to minion, where the tcp syn attack traffic on a standby is not blocked by blocker rule, though the DDOS is enabled.
Workaround	Disabling DDOS will bring the cpu back to normal.
Recovery	NA
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Layer 3 Routing/Network Layer

Issue	FI-267673
Symptom	In some scenarios, active DHCP snoop client's (v4 and v6) session information is not synchronized to the standby unit for full stack redundancy.
Condition	1. Enable DHCP snooping on configured VLANs 2. Bind the configured maximum allowed DHCP snoop clients 3. Reload stack or initiate switchover to standby
Workaround	No known workaround
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-267604
Symptom	Exec banner config is missing when system is idle for few days
Condition	Banner exec config displays only single line when system is idle for few days if multiple line banner exec configuration exists due to plugin restarts after config change related to clish.conf
Workaround	Delete and configure banner exec config
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-267286
Symptom	After upgrade from 8095 to 9010e, "banner motd require-enter-key" displays as "equire-enter-key".
Condition	Upgrade from 8095 to 9010e, "banner motd require-enter-key" configured.
Workaround	N/A
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Known Issues in Release 09.0.10d

Issue	FI-269875
Symptom	After stack switchover, the snmp-server group ACL rules are not working as expected
Condition	create snmp-server group ACL rule and execure Stack switchover
Workaround	None
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269787
Symptom	System up time shows incorrect value, when ICX acts as SNMP host and ICX event details updated in SNMP Server.
Condition	1. Configure snmp-server host v2c /v3 on ICX box. 2. Add host detail in SNMP server. 3. Create a event on ICX like create vlan.
Workaround	
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269760
Symptom	when deleting snmp-server community by using "no snmp-server/snmp-server" command, device may go on a reload..
Condition	Deletion on snmp-server community string configuration
Workaround	none
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269649
Symptom	After reload of 1 stack in MCT cluster, when the reloaded core comes up and joins the MCT cluster, not all traffic re-establishes.
Condition	When one stack in MCT cluster reloaded and joins the MCT cluster not all traffic re-establishes.
Workaround	
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269624
Symptom	When a SNMPv3 Request is sent from a user who does not have authorization for the requested OID, SNMP task restarts.
Condition	SNMPv3 Request done for an unauthorized OID
Workaround	None
Recovery	None.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-263984
Symptom	VRRPE interface config gets lost when upgrading.
Condition	VRRPE interface configs gets lost if multiple vrid's are configured on single interface.
Workaround	None
Recovery	Need to reconfigure again the lost config once the devices are up.
Probability	
Found In	FI 10.0.00
Technology / Technology Group	Layer 3 - VRRP and VRRP-E (IPv4)

Issue	FI-269588
Symptom	Crash is seen on executing "show ip vrrp-extended brief" when multiple vrids are configured on a single Virtual interface.
Condition	Device goes for reload on executing "show ip vrrp-extended brief" when multiple vrid's are configured on a single Virtual interface.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Layer 3 - VRRP and VRRP-E (IPv4)

Issue	FI-269554
Symptom	Unexpected restart of SNMP agent might happen when "show snmp server" is executed.
Condition	When snmp-server is configured with more than 17 hosts and "show snmp server" command is executed.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269540
Symptom	Crash is seen on executing "show ip vrrp-extended brief" when multiple vrids are configured on a single Virtual interface.
Condition	Device goes for reload on executing "show ip vrrp-extended brief" when multiple vrid's are configured on a single Virtual interface.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-269075
Symptom	Vrrp-e flap seen momentarily on MCT stack
Condition	Vrrp-e flap seen momentarily on MCT stack
Workaround	None
Recovery	
Probability	Low
Found In	FI 09.0.10
Technology / Technology Group	Layer 3 - VRRP and VRRP-E (IPv4)

Issue	FI-265941
Symptom	ISSU shows status as ISSU Abort while performing ISSU from 9010c to 9010d.
Condition	ISSU upgrade from 9010c to 9010d
Workaround	Image upgrade shall be performed using copy command instead of ISSU
Recovery	None
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	System - System

Issue	FI-265934
Symptom	Ping failed in Vxlan underlay/overlay configuration Topology
Condition	1. configure dut1 and dut3 as a overlay vxlan 2. dut4 and dut5 as underlay vxlan. 3. configure ospf between overlay to underlay. 4. then configure some loopback ip address in dut1 and dut3 5. try to ping the dut1 loopback ip address to dut3 its failed but dut1 to dut3 its ping
Workaround	None
Recovery	None
Probability	High
Found In	FI 09.0.10
Technology / Technology Group	Layer 2

Issue	FI-265878
Symptom	dhcp-server configuration pushed via SZ returns success from ICX, even though DHCP-client is enabled on the ICX
Condition	Configure DHCP-client on ICX. Configure DHCP Server Profile configuration on SZ and push it to ICX
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	Management - DHCP (IPv4)

Issue	FI-265867
Symptom	Customer will not be able to bring ICX in FIPS or FIPS-CC mode after modifying the configuration and followed by reload with 9010d Image
Condition	After migrating to 9010d, if we do write memory and followed by reload, ICX will come up with default configuration if ICX in FIPS or FIPS-CC mode.
Workaround	1. do the required configuration 2. write memory 3. copy startup-config tftp <server-ip> startup.cfg 4. copy tftp startup-config <server-ip> startup.cfg 5. Now reload the ICX
Recovery	None
Probability	High
Found In	FI 09.0.10
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-265796
Symptom	DNS server IP address set in a combination of DHCP and manual configuration after a reload doesnot apply the manually configured one
Condition	If both static and dynamic DNS server addresses are present in the configuration, saving the config and reloading the box , will not apply the manually configured server address
Workaround	After reload letting the DHCP server to push the DNS server IP address, followed by configuring the other DNS server address
Recovery	None
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	Management

Issue	FI-265793
Symptom	SSH crash during SZ connection in bad path or transition from good to bad path with poor network latency.
Condition	If device connected under good and bad environment with SZ, ICX device might encounter a SSH crash during bad path connection.
Workaround	None
Recovery	SSH crash will not reboot the ICX and the device will reconnect to SZ when the path moved to good path.
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	Management

Issue	FI-265725
Symptom	Duplicate LLDP neighbor are not shown on SZ, even though duplicate LLDP neighbors present and shown on ICX CLI ICX8200-24 Router(config)# show lldp nei Lcl Port Chassis ID Port ID Port Description System Name 1/1/12 609c.9f52.6f30 609c.9f52.5263 GigabitEthernet3/1/5 ICX7650-48P Router 2/1/14 609c.9f52.6f30 609c.9f52.9489 GigabitEthernet2/1/14 ICX7650-48P Router 2/1/47 0.0.0.0 1127493697 SW PORT SEPC40ACBE110A0 2/1/47 55.1.1.4 1127493697 SW PORT SEPC40ACBE110A0 2/1/48 0.0.0.0 943207745 SW PORT SEP885A92D9BAEA 3/1/1 609c.9f52.6f30 609c.9f52.6f30 GigabitEthernet1/1/1 ICX7650-48P Router ICX8200-24 Router(config)#
Condition	Have multiple LLDP neighbors for the same port
Workaround	None
Recovery	None
Probability	Low
Found In	FI 10.0.00
Technology / Technology Group	Management - LLDP - Link Layer Discovery Protocol

Issue	FI-265722
Symptom	Header field will be seen as remote MAC with SmartZone, in case of IPV4/ V6 and MAC address for lldp neighbors
Condition	Header filed as remote MAC is not correct as it may have IPv4, IPv6 and MAC address when different neighbors are connected.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 10.0.00
Technology / Technology Group	Management - LLDP - Link Layer Discovery Protocol

Issue	FI-265256
Symptom	priority-flow-control configuration on a priority group is removed after a reload
Condition	priority to priority group mapping (qos priority-to-pg) is configured. priority-flow-control is configured for any priority group. A reload is done.
Workaround	None
Recovery	Reconfigure the prioritiy-flow-control after reload.
Probability	Medium
Found In	FI 10.0.00
Technology / Technology Group	Traffic Management - Buffer Queue Management

Issue	FI-265634
Symptom	During stack switch-over, traffic loss will be seen if VLAN mirroring is enabled with PFC priority-to-pg group map configuration.
Condition	Customer will see Traffic loss in Mirrored traffic for few seconds during switch-over.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 10.0.00
Technology / Technology Group	Traffic Management - Buffer Queue Management

Issue	FI-265543
Symptom	Customer will not able to see the mac entries for the traffic from underlay to overlay using lag .
Condition	After migrating to 9010d, there will be no mac entries for the traffic from underlay to overlay using lag .
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	Layer 2

Issue	FI-265106
Symptom	Actual/expected webpage for example (www.cnn.com/health or www.cnn.com) is not opening after clicked the "Click here to go to your original location" which is after successful authentication.
Condition	Multiple webauth requests can cause success page is not to work
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	Security - Web Authentication

Issue	FI-263524
Symptom	Vlan mirroring is not happening for arp packets
Condition	Configure VLAN mirroring via CLI configuration
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 09.0.10 FI 08.0.95
Technology / Technology Group	Monitoring/RAS - Port Mirroring and Monitoring

Issue	FI-259980
Symptom	ARP refresh and traffic disruption seen though continuous traffic is received destined to the ARP entry
Condition	Configure ARP aging to 3 minutes. Send continuous traffic destined to the ARP entry
Workaround	None
Recovery	None
Probability	High
Found In	FI 09.0.10
Technology / Technology Group	Layer 2 - Topology Groups

Issue	FI-251663
Symptom	With 32k DHCP snoop entries, few entries are missing in "show ip dhcp snoop inf"
Condition	On ICX Router/Switch if dhcp snooping scale increases above 8k, we may see few dhcp snoop entries missing in dhcp snoop data base. And it can grow up till 500 entries when scale reaches maximum.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 09.0.10
Technology / Technology Group	System - CLI

Known Issues in Release 09.0.10c

Issue	FI-260716
Symptom	MACsec is not working between ICX peer with one have version FI 08.0.95 and other peer have FI 09.0.10
Condition	ICX software version must be one peer FI 08.0.95 and another peer FI 09.0.10
Workaround	No workaround
Recovery	NA
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-260551
Symptom	snmpisowalk fails with "Error: OID not increasing:"
Condition	while executing the OID SNMPv2-SMI::enterprises.1991.1.1.3.3.5.1.2.0
Workaround	Not Available
Recovery	Not Available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-260542
Symptom	Show monitor command doesnt return the desired output
Condition	When Configured the Monitor port
Workaround	Not Available
Recovery	Not Available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-260299
Symptom	Argument field in "show rmon event", will be displayed wrongly as '', when its not configured.
Condition	When event description is configured with MAX length (80) value
Workaround	Not Available
Recovery	Not Available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-260285
Symptom	The logTime object in logTable displays wrong time, which is not in sync with "show rmon log" output.
Condition	When log is generated for any rmon event
Workaround	Check "show rmon log" CLI output
Recovery	Not Available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-259903
Symptom	some of the RMON configurations are not persistent after reload
Condition	When we have 2000 scaled RMON configurations in the device
Workaround	Not Available
Recovery	Not Available
Probability	
Found In	FI 10.0.00
Technology / Technology Group	

Issue	FI-259167
Symptom	PIM issue on ICX7450-48P
Condition	PIM REG acl not getting programmed
Workaround	Not Available
Recovery	Not Available
Probability	
Found In	FI 10.0.00
Technology / Technology Group	

Known Issues in Release 09.0.10b

NOTE
Additional information, including conditions, workarounds, and recovery, will be added to tables missing these fields in an update to known issues in the next document revision.

Issue	FI-258753
Symptom	SNMP iso walk times out at “ruckusDhcpv6SnoopIfConfigTrustValue”.
Condition	Running SNMP Iso Walk on any Switch Build or Spatha Router Build
Workaround	None
Recovery	None
Probability	High
Found In	FI 09.0.10
Technology / Technology Group	SNMP / L3 VxLAN

Issue	FI-258622
Symptom	DHCP Snooping: DHCP clients fail to get address when broadcast flag is enabled
Condition	
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-258535
Symptom	No error message shown for failure when configuring virtual-link in OSPFv3
Condition	
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Layer 3 Routing/Network Layer - OSPFv3 - IPv6 Open Shortest Path First

Issue	FI-258458
Symptom	OSPF area config not show under running config in spite of the CLI prompt complaining about duplicate entry
Condition	
Workaround	
Recovery	
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	Layer 3 Routing/Network Layer - OSPFv3 - IPv6 Open Shortest Path First

Issue	FI-258295
Symptom	No error message shown for failure when configuring stub area in OSPFv3
Condition	
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.00
Technology / Technology Group	Layer 3 Routing/Network Layer - OSPFv3 - IPv6 Open Shortest Path First

Issue	FI-258075
Symptom	DOM (Optical Monitoring) may not work on Down Ports
Condition	User has an option to enable optical monitoring on Down ports so that even with optics inserted or cable connected, DOM can display the data. However in 9010b we may not have data but instead will observe "Optical monitoring threshold is in progress, please try later".
Workaround	None
Recovery	None
Probability	High
Found In	FI 09.0.10
Technology / Technology Group	Monitoring - Hardware Monitoring

Issue	FI-257416
Symptom	SSL profile error "Error - SSL profile is must for Dot1x/Mac-auth/Web-auth" ICX7550-48 Router(config-ssl-cloudpath)#radius-server host 10.176.166.42 ssl-auth-port 2083 profile cp_interim3 default key 0 $VSFALW5k dot1x mac-auth web-auth Error - SSL profile is must for Dot1x/Mac-auth/Web-auth
Condition	SSL profile error when configuring RADIUS server host under user profile node.
Workaround	Avoid configuring RADIUS server host under user profile node which is not supported
Recovery	NA
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-248619
Symptom	Unexpected system reboot when configuring port monitoring on a LAG member port
Condition	System may reboot when configure port monitoring with large (100+) LAG group IDs
Workaround	Avoid monitoring LAG ports when configure huge LAG Groups
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Port Mirroring and Monitoring

Issue	FI-239865
Symptom	Banner is not be displayed in Telnet, SSH, or Console session during login.
Condition	Banner needs to be configured and switchover needs to be initiated
Workaround	No workaround available
Recovery	Reconfigure banner
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Known Issues in Release 09.0.10a

Issue	FI-255326
Symptom	CLI shell application may crash during long run execution. No Functional or Traffic impact will be observed.
Condition	In stacking setup CLI shell application may crash during long run execution.
Workaround	Not available
Recovery	CLI shell application will be started automatically when doing login next time.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	System - CLI

Issue	FI-255067
Symptom	An incorrect value would be displayed in the output of snmpget/snmpwalk over snVrrpVirRtr2Entry table for the below oid. 1.3.6.1.4.1.1991.1.2.12.5.1.1.10 snVrrpVirRtr2IpAddrMask
Condition	1)router vrrp is configured on an ICX device and is activated on a interface. 2)snmpwalk operation is performed for snVrrpVirRtr2Entry table. 3)snmpget operation is performed for snVrrpVirRtr2IpAddrMask oid.
Workaround	No Work-around
Recovery	No Recovery
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-254721
Symptom	On 7850/7550/7650 ,port going to err disabled state before reaching threshold value.
Condition	pass the traffic with the large threshold value that is greater than redbyte value count after expiration of log timer for the port on which BUM suppression is configured.
Workaround	BUM Suppression by PPS can be used on these devices.
Recovery	no recovery
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-253934
Symptom	Network deployment were MAC movements across LAG interfaces are expected, traffic disruption for at-most MAC age period shall be observed upon Layer-2 forwarding path realignment.
Condition	Traffic forwarding gets black-holed for MAC age period on network were MAC moves between LAG interfaces.
Workaround	Network deployment to avoid unintentional MAC movements involving LAG interfaces
Recovery	Issue "clear mac-address" command on vlan/interface/system level will resume traffic forwarding
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-253904
Symptom	Removing the breakout configuration cannot be done at the top level port (ex: 1/2/1)
Condition	When breakout is configured, the removal cannot be done using the top level port. It needs to be done with the first breakout port
Workaround	Breakout can be removed using the first broken out port (1/2/1:1)
Recovery	None needed.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-253194
Symptom	i. snmpwalk of lldpStatsRxPortTable is not displaying the OID instances of "ICX7550-100G 2-port 200G Module" ii. snmpget of "ICX7550-100G 2-port 200G Module" OID instance for lldpStatsRxPortTable entries displays "No Such Instance currently exists at this OID"
Condition	when the snmpget/snmpwalk is done for lldpStatsRxPortTable in "ICX7550-100G 2-port 200G Module"
Workaround	'show lldp statistics' displays the table entries.
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251663
Symptom	on ICX Router/Switch full scale of dhcpsnoop entries (i.e.32k), around 500 entries are missed in the snoop table. But these IPs are allocated to those respective clients successfully. If Dynamic Arp Inspection is enabled on this box, ARP packets from those clients will be denied and reachability for those clients will be impacted.
Condition	on ICX Router/Switch if dhcp snooping scale increases above 8k, we may see few dhcp snoop entries missing in dhcp snoop data base. And it can grow up till 500 entries when scale reaches maximum.
Workaround	There is no workaround. Reduce the dhcp snoop scale and those missing entries would come back in the table.
Recovery	no recovery.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251512
Symptom	SNMPagentd process may crash when Large ACLs are configured.
Condition	When snmpbulkwalk is executed with large ACL configured in the device
Workaround	Not available
Recovery	snmpagentd will be retarted and available after the crash dump was colleected
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-248869
Symptom	Standby goes for one more reload when system-max " ip-route-default-vrf " is reset to default-value(ie Device is booted with a non-default value) and is reloaded again.
Condition	1)The ICX device should be a stack supporting forwarding-profile.
Workaround	No Work-around
Recovery	No Recovery
Probability	High
Found In	FI 09.0.10
Technology / Technology Group	Layer 3 Routing/Network Layer - IP Addressing

Known Issues in Release 09.0.10

Issue	FI-251641
Symptom	The fi_cli_shell process crashes when scanned with portscanner application.
Condition	When ports of the ICX device is scanned with portscanner for few hours
Workaround	
Recovery	CLI shell will be automatically restarted.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251868
Symptom	Strom Control Packet Per Second Rate limit wont work on Sica and Spatha
Condition	BUM Rate limit PPS config
Workaround	Storm Control Kbps can be used to achieve rate limit
Recovery	No Recovery
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251839
Symptom	In ICX7550 platform, CPU usage increases up to 60%.
Condition	The CPU high is seen in below conditions 1. when restconf is enabled in the device the CPU usage is 60% 2. when restconf is disabled the CPU usage is 40%
Workaround	Not available
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251793
Symptom	Host routes programmed in hardware not displayed in show hardwre route command.
Condition	In Minions, some of the ipv4 and ipv6 host routes programmed in hardware are not disalyed in "show hardware route devie 0" and "show hardware ipv6-route device 0" command.
Workaround	sh ip cache, or dm commands can be used to check the host routes
Recovery	sh ip cache, or dm commands can be used to check the host routes
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251663
Symptom	With full scale of dhcpsnoop entries (i.e.32k), around 500 entries are missed in the snoop table. But these IPs are allocated to those respective clients successfully. If Dynamic Arp Inspection is enabled on this box, ARP packets from those clients will be denied and reachability for those clients will be impacted.
Condition	When scale increases above 8k, we might see few snoop entries not learnt in snoop table. And it can grow up till 500 entries when scale reaches maximum.
Workaround	There is no workaround. Reduce the scale and those missing entries would come back in the table.
Recovery	no recovery.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251655
Symptom	snmpwalk on DHCP SERVER MIBs may get timeout response
Condition	when dhcp server pool is configured
Workaround	snmpwalk of DHCP server MIBs with timeout of 5 seconds
Recovery	snmpwalk of DHCP server MIBs with timeout of 5 seconds
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Cloud Management - Cloud Agent

Issue	FI-251653
Symptom	The snDhcpServerPoolOptionIPString returns empty string for option 21 and 33
Condition	When option 21 and 33 are configured in the dhcp server pools
Workaround	Not Available
Recovery	Not Available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251600
Symptom	We are seeing dhcpv4/dhcpv6 snoop entries not getting printed fully in serial console when show-command is given. Only 5k entries are getting printed in the serial console. But show-command from ssh/telnet session prints all the entries. There is no functionality impact with this.
Condition	We see this printing issue in serial console when dhcpv4/dhcpv6 snoop entries increases above 5k. This issue is not there when show-command is given from telnet or ssh session.
Workaround	use ssh/telnet session instead of serial console.
Recovery	on recovery.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-251546
Symptom	Stale supportsave operation details which suggest successful or failure or cancel operation performed after a fresh/re-login.
Condition	1. login to webui and execute SS 2. logout of web 3. login again and navigate to Infra
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251542
Symptom	In WebUI on successful execution of 'Supportsave all' or 'Supportsave core' operation, older core files are not deleted
Condition	Trigger 'Supportsave all' or 'Supportsave core' operation from WebUI
Workaround	Trigger 'Supportsave all' or 'Supportsave core' operation from cli
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251540
Symptom	Doing Supportsave operation from WebUI is generating 2 core files while supportsave operation from CLI generates 1 core file.
Condition	Login to webui and execute Supportsave operation
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251534
Symptom	User will not be able to enter to priveleged mode when telnet to the device throgh revSSH tunnel from SZ CLI
Condition	The issue happens only when aaa authorization with tacacs configured aaa authorization exec default radius tacacs+ aaa authorization commands 0 default radius tacacs+
Workaround	Not Available
Recovery	If AAA authorization through TACACS+ server configuration is removed
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Cloud Management - Cloud Agent

Issue	FI-251512
Symptom	SNMPagentd process may crash when Large ACLs are configured.
Condition	When snmpbulkwalk is executed with large ACL configured in the device
Workaround	Not available
Recovery	snmpagentd will be retarted and available after the crash dump was colleected
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251481
Symptom	Multicast control packets (e.g IGMP packets) are not filtered by mirror filter
Condition	When mirroring is configured (either by mirror port or by RSPAN), and mirror filtering is configured on the source vlan Id, mirror filter is not filtering the multicast control packets of that Vlan
Workaround	Not available
Recovery	Recovery not available in this release
Probability	
Found In	FI 09.0.10 FI 08.0.90 FI 08.0.95
Technology / Technology Group	

Issue	FI-251462
Symptom	DOT1X client's IPv6 address is not updated successfully during snmpget with MIB object <ruckusWiredClientV6Addr>.
Condition	Authenticated DOT1X client with IPv6 address should exist
Workaround	Fetch IPv6 address of authenticated DOT1X client using MIB object <ruckusAuthSessionAddr>
Recovery	Recovery not applicable
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251404
Symptom	'show ipv6 dhcp6-server lease' command displays the lease entry in active state even when the lease entry is release
Condition	After the lease entries are expired/released
Workaround	Not available
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-223420
Symptom	With RSPAN feature enabled to mirror egress traffic, The BPDU control packets are not excluded from mirroring.
Condition	Configure "rspan source monitor-out ethernet < >" under rspan vlan on ICX Switch or Router.
Workaround	No Workaround
Recovery	No Recovery
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-250871
Symptom	Edge devices such as laptops may lose network connectivity with frequent MAC address operations (add/delete).
Condition	The network connectivity may be affected with frequent MAC operations - MAC address add/delete.
Workaround	Reducing the MAC operations via Solar Winds monitoring app.
Recovery	Switch reload should recover the unit.
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Layer 2 Switching - VLAN - Virtual LAN

Issue	FI-251292
Symptom	In ICX with stack enabled, 1. on reload, error message "Error [1 1] parsing line:" is displayed for alias commands in the standby unit 2. On failover/switchover of the stack unit, in new active unit, alias commands will not be available and it will not be working
Condition	In ICX with stack enabled on reload of the device
Workaround	Not available
Recovery	Configure the alias commands after stack switchover/failover of the device
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251284
Symptom	clear ipv6 dhcp6-server binding * is not deleting the dhcpv6 lease entries
Condition	when more than one dhcpv6 lease entry is present
Workaround	Remove the lease entries one by one
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251203
Symptom	Mirror filter configuration not rejected when ACL mirroring is conifgured
Condition	when ACL based mirroring is configured, mirror filter configuration is allowed.
Workaround	workaround not available for this issue
Recovery	Recovery not available for this issue
Probability	
Found In	FI 09.0.10 FI 08.0.95
Technology / Technology Group	

Issue	FI-251146
Symptom	Not possible to modify the rspan-transit vlan.
Condition	When rspan-transit vlan is configured , will not be able to modify the transit vlan like changing the vlan member ports.
Workaround	rspan-transit vlan can be deleted and added again with new configurations
Recovery	rspan-transit vlan can be deleted and added again with new configurations
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-245658
Symptom	When vlan is added to the group-vlan after the creation of group-vlan, the ping across group-vlans fail.
Condition	The ping fails only when vlan is added to the group-vlan after vlan-group creation. If vlan is added as part of group-vlan creation itself, it pings successfully.
Workaround	
Recovery	Issue gets recovered on deleting and re-adding of the group-vlan ip address. Another way is to delete the group-vlan and re-create it with all vlans specified as part of creation itself.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-250487
Symptom	Agent System Config Load config via SNMP is currently not supported. For sample: The following SNMP Set is not supported snmpset -v2c -c public 10.177.121.76 1.3.6.1.4.1.1991.1.1.2.1.9 i 24 (uploadFromFlashToNMS) snmpset -v2c -c public 10.177.121.76 1.3.6.1.4.1.1991.1.1.2.1.9.0 i 26 (uploadFromDramToNMS)
Condition	Not Applicable
Workaround	Use CLI for running the commands instead.
Recovery	Not Available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-250280
Symptom	User may experience that the end devices get IP address [through DHCP or otherwise] but cannot reach the internet and devices on local network.
Condition	User may experience the symptom in a highly scaled environment with thousands of end devices such as PCs/laptops etc.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

Issue	FI-250305
Symptom	Forwarding between VLANs in group fails after adding new VLAN to group
Condition	Forwarding fails only when vlan is added to the group-vlan after vlan-group creation. If vlan is added as part of group-vlan creation itself, it works successfully.
Workaround	
Recovery	Issue gets recovered on deleting and re-adding of the group-vlan ip address. Another way is to delete the group-vlan and re-create it with all vlans specified as part of creation itself.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-250295
Symptom	The lldp civic address is not displayed in 'show lldp local-info' and 'show lldp neighbors'
Condition	when lldp civic address is configured
Workaround	The details are displayed in the running configuration 'show run'
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-249452
Symptom	The ICX device is not switchover back to the new active SZ cluster once the failover to backup SZ cluster is complete.
Condition	New SZ active cluster is sent to ICX device after failover to backup cluster
Workaround	None
Recovery	configure 'no manager active-list' manually from ICX
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-250283
Symptom	Cloud LED is blinking continuously
Condition	when the switch connected to SZ the cloud LED is blinking continuously
Workaround	Not available
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-250247
Symptom	No cli output is seen or sometime garbage letters observed in webcli output in WebUI
Condition	run cli commands in webcli from WebUI
Workaround	enable 'skip-page-display'
Recovery	enable 'skip-page-display'
Probability	
Found In	FI 09.0.10 FI 04.0.00
Technology / Technology Group	

Issue	FI-249479
Symptom	snAgentCpu OID was not working for ICX 7550
Condition	Issue was observed while doing snmpwalk/snmpget for snAgentCpu OID
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-249788
Symptom	PFC frames are not sent out in case of congestion and traffic is not reduced
Condition	Traffic congestion on PFC enabled priority
Workaround	Configure flow control
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-249651
Symptom	SNMP and CLI output mismatch for lldpLocSysDesc and lldpRemSysDesc OID
Condition	when LLDP neighbors has system description advertised
Workaround	Not available
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-249375
Symptom	MCT client has ospf neighborship with both MCT cluster peers and it learns a route prefix (say X) from both peers. When the entire MCT cluster (i.e. both peers) are reloaded and then icl link is disabled, route for prefix X gets removed from mct client's route table. It is re-learned in few seconds. During this time of ospf route deletion and addition temporary traffic drop can be seen and it can be upto 1 minute.
Condition	This issue will be seen only when icl link is disabled for the first time. After that icl disable/enable doesn't create this problem
Workaround	
Recovery	Issue recovers after ospf route is re-learned
Probability	
Found In	FI 09.0.10
Technology / Technology Group	IP Multicast - IPv4 Multicast Routing

Issue	FI-249335
Symptom	"show ip multicast mcache" and "show ip multicast group" commands does not display complete output in scale scenario
Condition	When 'skip-page-display' is enabled "show ip multicast mcache" and "show ip multicast group" complete output is not displayed
Workaround	use paged mode display to see complete output
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-249281
Symptom	"show lldp neighbors detail" doesn't show the details of all the neighbors in scaled scenario. "show lldp neighbors", doesn't show all the neighbors in scaled scenario.
Condition	In scaled LLDP scenario not all neighbors are shown in "show lldp neighbors" and "show lldp neighbors detail" cmds
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-249198
Symptom	
Condition	On an MCT setup, IGMP/MLD snooping is enabled on 99 VLANs. When all lags connected to CCEP clients are disabled, traffic drop has been observed.
Workaround	Limit the VLANs to less than 99
Recovery	Stop the traffic and reload the MCT node
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-249127
Symptom	The below syslog is continuously displaying on the ICX when the device is not connected to SZ, SYSLOG: <14> Sep 22 07:54:33 tanto MGMT Agent: Connected to network controller at 10.176.187.194
Condition	When i. configured the ssh port on SZ to "26" and ii. configured manager ssh port on ICX to 25
Workaround	Configure the same port as ssh port in both SZ and ICX
Recovery	Configure the same port as ssh port in both SZ and ICX
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-199793
Symptom	Core file is not generated when ICX7650 reloads unexpectedly.
Condition	When ICX7650 reloads unexpectedly due to kernel crash, the core file is not generated.
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.92
Technology / Technology Group	System - System

Issue	FI-248836
Symptom	IPV6 management address details wont be seen in snmpwalk output of lldpRemManAddr table
Condition	SNMP walk/get operations are not fetching output for IPv6 management address in lldpRemManAddr table
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-248614
Symptom	RTM has not learnt all the OSPF routes.
Condition	Continuous network flap could lead to aging out of network LSA, in turn leading to route calculation abort.
Workaround	None
Recovery	Retriggering route calculation. Suggested method by modifying the OSPF cost on one of the OSPF interfaces.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-247980
Symptom	Mirror filter is not filtering traffic from the source vlan configured for mirror filter
Condition	The issue is present in the BCM devices DD3 HX5 series.
Workaround	Workaround not available
Recovery	Recovery not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-247951
Symptom	On copying a random/incorrect config file, the parsing failed internally but no errors are displayed on the UI.
Condition	Download of an invalid config file will result in triggering the above issue.
Workaround	Download of the correct config file after failure.
Recovery	Download of the correct config file after failure.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-240811
Symptom	While loading the mib file in NNMi mib browser tool, It throws some standard errors.
Condition	While loading the mib file in NNMi mib browser tool, It throws some standard errors.
Workaround	
Recovery	None
Probability	
Found In	FI 08.0.70 FI 08.0.90 FI 08.0.95
Technology / Technology Group	

Issue	FI-247430
Symptom	SNMP walk displaying "OID not increasing" error when initiating walk over lldpLocManAddrTable table
Condition	Configure Ipv6 address for lldpLocManAddrTable table and perform snmp walk.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-247023
Symptom	User allowed to bind Egress ACL when ACL's filter has "internal-priority-marking" via SZ .
Condition	When ACL's filter has "internal-priority-marking" configured via SZ
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-246840
Symptom	SNMPwalk/bulkwalk operation for LLDP MED non-accessible OID lldpXMedRemLocationInfo displays 'No such instance' message
Condition	when lldp location is configured for lldp neighbors
Workaround	The cli command 'show lldp neighbors' will display the lldp location information
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-246821
Symptom	Below errors may seen in console of the ICX 7850 : 1. sh: /.pkg/httpPkg/util/hmon_nginxfmntr: cannot execute binary file: Exec format error 2. /.pkg/httpPkg/bin/curl: symbol lookup error: /.pkg/httpPkg/lib32/libcurl.so.4: undefined symbol:
Condition	In an idle 7850 device
Workaround	Not available
Recovery	Not available
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-231152
Symptom	In 'show ip address' output, the dynamic ip address lease time displays N/A for sometime (about 90secs). Then it updates with lease time.
Condition	After stack switchover, in 'show ip address' output the dynamic ip address lease time displays N/A for sometime (about 90secs). Then it updates with lease time. DHCP Renewal doesn't happen after switchover only rebinding happens.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-242893
Symptom	Show command "sh mac access-lists bri | i Total ACL count" is taking 30 secs to display the output.
Condition	when maximum mac acl's are configured in the device
Workaround	Not available
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

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

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-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-241498
Symptom	After stack failover or switchover, Vxlan traffic forwarding will not be operational, if the traffic is arriving at the slave unit, if previous Vxlan unconfigure operation hadn't happened in a particular order.
Condition	Execute no lag(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-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-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-242556
Symptom	Duplicate DHCPACK packets are received in the DHCP client
Condition	When an ICX relay device is present in between DHCP client and server
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-226544
Symptom	dhcp client i. 'show ip dhcp-client options' may not display the option values received from dhcp server correctly ii. 'show ip dhcp-client options' may not display the option 12 value correctly dhcp server iii. The DHCP ACK and offer packets received by dhcp client may have wrong padding bytes
Condition	dhcp client i. When special characters are configured in dhcp options in the dhcp server ii. when more than one word is configured in option 12 in dhcp server dhcp server iii. when the configured options length module 4 is not zero
Workaround	None
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-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-233642
Symptom	With TACACS+ server accounting enabled on device, on verification of accounting logs in TACACS + server. The TACACS+ accounting logs doesn't display time zone information.
Condition	This symptom is seen with TACACS+ accounting
Workaround	Not available
Recovery	Not available
Probability	
Found In	FI 09.0.00
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 09.0.10 FI 08.0.95
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-241568
Symptom	On enable command "Error - Config send failed" error is seen with AAA enable authentication after upgrade to 9010
Condition	configure more than 4 tacacs+ server host and the reachable server should be 5th or more in the list.
Workaround	The reachable tacacs+ server host is less than or equal to 4 in the list the issue does not occur
Recovery	Change the reachable tacacs+ server order in the list to less than or equal to 4
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 logins 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-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	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-239517
Symptom	SNMP operation on below tables will fail. 1) lldpXdot1RemProtoVlanSupported 2) lldpXdot1RemProtoVlanEnabled 3) lldpXMedLocalData In snmp v1 traps invalid source ip addres is observed
Condition	Below SNMP tables are not supported 1) lldpXdot1RemProtoVlanSupported 2) lldpXdot1RemProtoVlanEnabled 3) lldpXMedLocalData Invalid source ip observed in snmp v1 traps
Workaround	None
Recovery	None
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-237257
Symptom	No configuration provision for access mode (enable/login/webserver/snmp) available when configuring AAA authentication method using Restconf
Condition	When using Restconf for configuring AAA authentication method
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-233642
Symptom	With TACACS+ server accounting enabled on device, on verification of accounting logs in TACACS + server. The TACACS+ accounting logs doesn't display time zone information.
Condition	This symptom is seen with TACACS+ accounting
Workaround	Not available
Recovery	Not available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-199753
Symptom	Hostname configured statically through CLI will be overwritten by hostname received through DHCP messages.
Condition	1. Configure the hostname through CLI in ICX. 2. Configure the different hostname for clients at DHCP server. 3. hostname will be replaced once ICX receives the offer message from DHCP server.
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Layer 3 Routing/Network Layer - DHCP - Dynamic Host Configuration Protocol

Issue	FI-251920
Symptom	When MCT is provisioned, under scaled condition with line rate traffic during longevity - Active unit may crash due to some unknown heap memory corruption and will trigger failover.
Condition	When MCT is provisioned under scaled condition.
Workaround	No workaround at this moment
Recovery	Not required because stack failover will recover the system.
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-251923
Symptom	MCT Stacking: EPCL ACL rules are missing for the unit when unit goes down and rejoins stack.
Condition	
Workaround	No workaround at this moment
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-260112
Symptom	When a multiple line banner message is configured from SZ, all the lines in the message do not get configured due to the input string not being in the expected format, and an error message does not get displayed for the same.
Condition	When a multiple line banner message is configured from SZ using cli template and if each line except the last line is not terminated with ^C.
Workaround	
Recovery	When configuring from SZ, terminate each line except the last line in the banner string with ^C character
Probability	
Found In	09.0.10
Technology / Technology Group	

Closed Issues with Code Changes in Release 09.0.10e

Issue	FI-269554
Symptom	Unexpected restart of SNMP agent might happen when "show snmp server" is executed.
Condition	When snmp-server is configured with more than 17 hosts and "show snmp server" command is executed.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-266764
Symptom	Unexpected reload of ICX device might happen
Condition	1. DHCP6 Helper address configured in any of the ICX interface 2. DHCP6 Relay forward packet received in an ICX interface where there is no explicit helper address.
Workaround	None
Recovery	
Probability	Low
Found In	FI 08.0.92
Technology / Technology Group	Layer 3 Routing/Network Layer - DCHP IPv4/IPv6 Relay

Issue	FI-268518
Symptom	Changing the hostname breaks webGUI access
Condition	While reading the hostname through SHMdb, it fails due junk values in python read. Added ITC to get the hostname from get_hostname_value function which is in ui_be_hostname.c file.
Workaround	changing the hostname from webui/CLI will reflect the new hostname in the CLI and also updates the webpage title with new hostname after "reloading the web page".
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Management - Management GUI

Closed Issues with Code Changes in Release 09.0.10e

Issue	FI-268239
Symptom	Unexpected Device reload might be observed in ICX7850 platform.
Condition	Issue specific to ICX7850 Megamind platform. While ARP and neighbors are learnt in the system, 1. Remove the interface from the Vlan. 2. Delete the vlans which has tagged ethernet interface.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 09.0.10
Technology / Technology Group	System - System

Issue	FI-267565
Symptom	Unexpected reboot might be experienced on 7250/7150 devices
Condition	Unexpected reboot might be experienced on 7250/7150 devices when a packet is is received and processed by the CPU
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Other - Other

Issue	FI-266766
Symptom	Firmware version is not displayed correctly on WebGUI.
Condition	Firmware version is not displayed correctly on WebGUI.
Workaround	NA
Recovery	NA
Probability	
Found In	FI 09.0.00
Technology / Technology Group	Management - Management GUI

Issue	FI-266467
Symptom	Interface with IPv6 configured might not come up after warm/cold restart if IP FOLLOW command is configured on the VE along with IPv4.
Condition	Configure ip follow configuration for any interface. Configure ipv4 and ipv6 addresses on the same interface.
Workaround	
Recovery	After device boot up, If we remove ip follow configuration from the the interface running configuration, interface's ve port status will be up. Alternatively, if physical port is administratively made down and up, the interface will come up.
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - IPv6 Addressing

Issue	FI-265703
Symptom	If DHCP session is terminated from the DHCP server and if DHCP client requests new IP after lease expiry, IP address will be assigned and connectivity (ping to DHCP server) might be lost when source guard is configured.
Condition	When DHCP session is terminated from the DHCP server and then when lease expires , connectivity from DHCP client to server might be lost
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Security - IP Source Guard

Issue	FI-266266
Symptom	OSPF Routing not working when connectivity lost between the devices.
Condition	OSPF Routing Enabled and Routing table have 300 external routes imported in NSSA area.
Workaround	
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - OSPFv3 - IPv6 Open Shortest Path First

Issue	FI-266250
Symptom	snmpwalk returns same iftype for normal and lag interfaces
Condition	snmpwalk returns same iftype for normal and lag interfaces
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-266302
Symptom	ICX Syslog event has Critical severity for RADIUS Accept events.
Condition	
Workaround	No workaround
Recovery	Refers to only the severity of the Syslog event; no recovery is necessary.
Probability	
Found In	FI 09.0.00
Technology / Technology Group	

Issue	FI-263500
Symptom	After reload /power cycle /switch-over, LAG ports adding validation might fail if BUM is configured.
Condition	When both Lag ports and BUM are configured
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Layer 2 Switching - LAG - Link Aggregation Group

Issue	FI-264365
Symptom	Customer unable to configure command speed-duplex 10-half as BCM error is observed.
Condition	When configured speed-duplex 10-half via configuration mode on an ethernet interface.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Closed Issues with Code Changes in Release 09.0.10d

Issue	FI-262110
Symptom	When Customer move the AP's over to the 7550s they're seeing AP's hit a PD Overload state and go offline
Condition	There is high inrush current with R650 AP when connected to 4pair poe port.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Other - Other

Issue	FI-261142
Symptom	Unexpected reload of the ICX will be observed when a filter is applied to the redistribution from BGP to OSPF using a distribute-list and a route map
Condition	Unexpected reload of the ICX will be observed when a filter is applied to the redistribution from BGP to OSPF using a distribute-list and a route map
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Security - PBR - Policy-Based Routing

Issue	FI-262408
Symptom	System started time might be drifting in the output of "show version" command.
Condition	Output of "show version" CLI has System start time which keeps changing continuously.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.95
Technology / Technology Group	Other - Other

Closed Issues with Code Changes in Release 09.0.10d

Issue	FI-262243
Symptom	ssh might fail with mngt vrf set and mngt acl applied.
Condition	ssh might fail with mngt vrf set and mngt acl applied.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	Management

Issue	FI-261257
Symptom	High CPU might be observed because of ssh session being closed abnormally.
Condition	When SSH session is closed abnormally and the show CLI command output displayed partially in page mode.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 09.0.10
Technology / Technology Group	Other - Other

Issue	FI-261062
Symptom	Help string of the DHCP server CLI "Lease count" is not very clear
Condition	None
Workaround	None
Recovery	None
Probability	Low
Found In	FI 10.0.00 FI 09.0.00 FI 10.0.10
Technology / Technology Group	Management - CLI - Command Line Interface

Issue	FI-261055
Symptom	DHCP server is not set static IP mappings based on the physical port configured.
Condition	DHCP server to reserve static IP Address for Physical port.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	Management - DHCP (IPv4)

Issue	FI-258438
Symptom	Unable to reach ICX from Gateway when VLAN mirroring is configured on the VLAN.
Condition	Issue is specific to ICX 7150. When VLAN mirroring is configured on the VLAN connected to Gateway, ARP Request packets are dropped.
Workaround	None
Recovery	1. Clear ARP corresponding to Gateway in ICX 2. Ping Gateway from ICX
Probability	Medium
Found In	FI 09.0.10 FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

Issue	FI-260023
Symptom	Device might experience unexpected reload while processing TCP based communication close operation.
Condition	When any TCP based application closes the connection, device might experience unexpected reload rarely.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.95
Technology / Technology Group	Cloud Management

Issue	FI-259907
Symptom	Device might reload unexpectedly when interface is configured with secondary ip address and primary address is replaced with dynamic option.
Condition	1. Configure primary and secondary ip address for an interface. 2. In the same interface try to change the primary ip address with dynamic and replace option. (e.g.,) sdwcore(config-if-e10000-2/1/1)# ip address <new ip> <netmask> dynamic replace
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Stacking - Traditional Stacking

Closed Issues with Code Changes in Release 09.0.10d

Issue	FI-260223
Symptom	While upgrading to 9010b, the SSH keys have to be regenerated in order for the SSH server to be enabled.
Condition	Upgrade to 9010b
Workaround	None
Recovery	None
Probability	High
Found In	FI 09.0.10
Technology / Technology Group	System - CLI

Issue	FI-260225
Symptom	Unexpected reload might be observed during LLDP configuration
Condition	System observed unexpected reload when LLDP neighbor details are fetched and displayed
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 09.0.10
Technology / Technology Group	System - CLI

Issue	FI-252107
Symptom	Active Unit might be Frozen and standby unit will not take over.
Condition	Active Unit might be Frozen and standby unit will not take over.
Workaround	None
Recovery	Power cycle the active unit
Probability	Medium
Found In	FI 08.0.90
Technology / Technology Group	Stacking - Traditional Stacking

Issue	FI-255593
Symptom	Unexpected reload of the device might be experienced in ICX 7250.
Condition	Unexpected reload of the device can happen when processing incoming packet.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Stacking - Stack Management

Issue	FI-255806
Symptom	Ping to VRRP IP fails when ACLs are applied on the VLAN.
Condition	The issue occurs when ACLs are applied to the VLAN.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 - VRRP & VRRP-E (IPv4)

Issue	FI-255299
Symptom	When VRRP-E is configured on a VE, the ICX device will take up the main role even though , if it has the "active Backup" command configured.
Condition	1. Set the track-ports on the Vrrp-e in master device and then "activate backup". 2. Reload the device. The Unit comes back as the Master from Backup.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - VRRPv2 - Virtual Router Redundancy Protocol Version 2

Issue	FI-254961
Symptom	ICX7550 may sometimes report "PoE severe error: Lost communication link with the PoE controller" error.
Condition	ICX7550 may sometimes report "PoE severe error: Lost communication link with the PoE controller" error.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	Management - PoE/PoE+

Issue	FI-254184
Symptom	Unexpected reload of ICX might be experienced, when ACL logging is enabled.
Condition	When IPv4 ACL Logging is applied in ICX.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.95
Technology / Technology Group	Security - ACLs - Access Control Lists

Closed Issues with Code Changes in Release 09.0.10d

Issue	FI-254237
Symptom	TFTP image copy might fail with timeout error, when sflow is enabled with sample rate less than 1024.
Condition	When sflow is enabled and if tftp image copy is triggered, copy might fail when UDP packets are received in out-of-order.
Workaround	Set the sflow sample rate to 1024 or Higher.
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Management - sFlow

Closed Issues with Code Changes in Release 09.0.10c

Issue	FI-251827
Symptom	" show relative-utilization <list.no>" , will display counts properly
Condition	when traffic runs on configured ethernet ports
Workaround	Not Available
Recovery	Not Available
Probability	
Found In	FI 08.0.90 FI 08.0.95 FI 09.0.00
Technology / Technology Group	

Issue	FI-248619
Symptom	FI crash observed
Condition	when tried to use monitor "ethe-port-monitored <port>" under lag
Workaround	Not Available
Recovery	Not Available
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Closed Issues with Code Changes in Release 09.0.10b

Issue	FI-256884
Symptom	ICX hostname is showing with double quotes when pushed from SZ
Condition	1. switch hostname pushed from SZ
Workaround	None
Recovery	None
Probability	High
Found In	FI 09.0.10
Technology / Technology Group	Management - Configuration Fundamentals

Issue	FI-255377
Symptom	show media output has Garbled characters or empty fields.
Condition	1. SFP inserted in ICX Interface
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.90 FI 08.0.95
Technology / Technology Group	System - Optics

Issue	FI-252913
Symptom	Dm diag on ICX 7150 returns failure
Condition	CPU Packet Diagnosis failure for 10Gport
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-250161
Symptom	High CPU is observed
Condition	1.when 'multicast passive/active' is configured. 2. Inflow of Multicast traffic
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	

Closed Issues with Code Changes in Release 09.0.10b

Issue	FI-248899
Symptom	customer unable to save the running config and erase startup config
Condition	1. When saving running config and erasing startup config is done through SNMP.
Workaround	None
Recovery	None
Probability	High
Found In	FI 09.0.00
Technology / Technology Group	

Closed Issues with Code Changes in Release 09.0.10a

Issue	FI-252581
Symptom	Unexpected reload of ICX While processing ARP packet
Condition	Unexpected reload of ICX While processing ARP packet
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

Issue	FI-252809
Symptom	Switch may become unresponsive when 'ip default-network' command is configured.
Condition	Switch may become unresponsive when 'ip default-network' command is configured.
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Layer 3 Routing/Network Layer

Issue	FI-252032
Symptom	In sflow sample the outgoing VLAN value is set wrongly.
Condition	In sflow sample the outgoing VLAN value is updated with default VLAN value instead of the existing VLAN value.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.90 FI 08.0.95
Technology / Technology Group	

Issue	FI-251644
Symptom	ICX device running with 8095x code reloads unexpectedly.
Condition	ICX device might reload unexpectedly when a monitoring tool that periodically SSH into the ICX device, running with 8095x code, to collect ‘show arp’.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

Closed Issues with Code Changes in Release 09.0.10a

Issue	FI-250982
Symptom	system name displayed in the binary format in show lldp neighbor output when ICX is connected with other vendor devices
Condition	1. Connect ICX with other vendor devices(cisco/extreme) 2. Enable lldp 3. Execute show lldp neighbor command in ICX. System name would be displayed in binary format
Workaround	show lldp neighbor details CLI command output displays valid system name
Recovery	None
Probability	
Found In	FI 08.0.90 FI 08.0.95
Technology / Technology Group	

Issue	FI-251493
Symptom	DHCP option 43 value is not received correctly by the dhcp clients
Condition	when DHCP option 43 is configured as HEX or IP address in ICX acting as DHCP server
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.00 FI 09.0.10 FI 09.0.00
Technology / Technology Group	

Issue	FI-250969
Symptom	Upgrade from 8090 to 8095 and ICX will be losing connectivity to devices whose arp entries are configured statically with static ARP inspection feature turned on.
Condition	1. Add static ARP entry. 2. Enable static ARP inspection and authentication source-guard-protection at interface level
Workaround	Remove the authentication source-guard-protection enable at the interface level and add the source-guard to the VLAN and do source-guard binding.
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	Security - IP Source Guard

Issue	FI-250751
Symptom	ICX7150 has a small TCAM space for storing dynamic routes which is carved out to store IPv4 and IPv6 routes. In some cases more IPv4 routes are present and more space is needed and may not find space to program them.
Condition	The issue may occur when the router needs more TCAM space to store IPv4 routes than the carved out space.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - Static Routing (IPv4)

Issue	FI-245408
Symptom	Unable to configure bpdu-flood-enable command
Condition	Added support to enable bpdu-flood-enable command which was earlier supported in Marvel platforms only.
Workaround	No Workaround
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-250280
Symptom	User may experience that the end devices get IP address [through DHCP or otherwise] but cannot reach the internet and devices on local network.
Condition	User may experience the symptom in a highly scaled environment with thousands of end devices such as PCs/laptops etc.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

Issue	FI-240811
Symptom	While loading the mib file in NNMi mib browser tool, It throws some standard errors.
Condition	While loading the mib file in NNMi mib browser tool, It throws some standard errors.
Workaround	
Recovery	None
Probability	
Found In	FI 08.0.70 FI 08.0.90 FI 08.0.95
Technology / Technology Group	

Resolved Issues in Release 09.0.10

This section lists software issues with Critical, High, and Medium Technical Severity that were resolved with a code change in release 09.0.10.

Issue	FI-202413
Symptom	ICX7550 / ICX7650 / ICX7850 port connected to VDX will be down.
Condition	ICX7550 / ICX7650 / ICX7850 port connected to VDX will be down when connected with 1G SFP.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.70
Technology / Technology Group	System - Optics

Issue	FI-229697
Symptom	Unable to have uplink ports on regular and Primary PVLAN at the same time.
Condition	Will not be able to tag same port on regular and Primary PVLAN at the same time.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.80 FI 08.0.90
Technology / Technology Group	Layer 2 Switching - VLAN - Virtual LAN

Issue	FI-241626
Symptom	Portstate change to Blocked after adding VLAN on Interface
Condition	After adding the VLAN on an interface, the Port state changed to blocking
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-242588
Symptom	Most of the local IPS are lost after upgrading
Condition	After upgrading to 8095 we are observing some lose in IPS
Workaround	
Recovery	
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

Issue	FI-245145
Symptom	Block MCT feature on ICX7550- Godzilla platform.
Condition	Was able to configure MCT cluster on 7550, which was unsupported on this platform(ICX7550) and was misleading.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-242914
Symptom	Added support for LFS feature on LAG interface
Condition	Added support for LFS feature on LAG interface
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.70 FI 08.0.80 FI 08.0.92 FI 08.0.95
Technology / Technology Group	Monitoring - Hardware Monitoring

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 09.0.10 FI 08.0.95 FI 09.0.00
Technology / Technology Group	Layer 3 Routing/Network Layer - VRRPv2 - Virtual Router Redundancy Protocol Version 2

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com