

# FastIron 08.0.90f for Ruckus ICX Switches Release Notes Version 1

Supporting FastIron 08.0.90f

# Copyright, Trademark and Proprietary Rights Information

© 2020 CommScope, Inc. All rights reserved.

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

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex 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

---

<b>Document History.....</b>	<b>5</b>
<b>Introduction.....</b>	<b>7</b>
About FastIron Release 08.0.90.....	7
Document Feedback.....	7
Ruckus Product Documentation Resources.....	7
Online Training Resources.....	8
Contacting Ruckus Customer Services and Support.....	8
What Support Do I Need?.....	8
Open a Case.....	8
Self-Service Resources.....	8
<b>New in This Release.....</b>	<b>11</b>
Hardware .....	11
Ruckus ICX 7850 Switch.....	11
Important Changes in Release 08.0.90.....	12
Software Features.....	12
New Software Features in 08.0.90f.....	12
New Software Features in 08.0.90e.....	12
New Software Features in 08.0.90d.....	12
New Software Features in 08.0.90c.....	12
New Software Features in 08.0.90b.....	13
New Software Features in 08.0.90a.....	13
New Software Features in 08.0.90.....	13
CLI Commands.....	15
New Commands in 08.0.90f.....	15
New Commands in 08.0.90e.....	15
New Commands in 08.0.90d.....	15
New Commands in 08.0.90c.....	15
New Commands in 08.0.90b.....	15
Modified Commands in 08.0.90b.....	15
Deprecated Commands in 08.0.90b.....	16
New Commands in 08.0.90a.....	16
New Commands in 08.0.90.....	16
Modified Commands in 08.0.90.....	18
Deprecated Commands in 08.0.90.....	19
RFCs and Standards.....	20
MIBs .....	20
New MIBs in Release 08.0.90.....	20
<b>Hardware Support.....</b>	<b>21</b>
Supported Devices .....	21
Technical Support Advisory.....	21
Advisory Overview.....	21
Supported Power Supplies.....	22
Supported Optics.....	22
<b>Software Upgrade and Downgrade.....</b>	<b>23</b>

Image File Names.....	23
PoE Firmware Files.....	23
Open Source and Third Party Code.....	24
<b>Issues.....</b>	<b>27</b>
Closed with Code Changes in Release 08.0.90f.....	27
Closed with Code Changes in Release 08.0.90e.....	33
Closed with Code Changes in Release 08.0.90d.....	36
.....	36
Closed with Code Changes in Release 08.0.90c.....	39
Closed with Code Changes in Release 08.0.90b.....	51
Closed with Code Changes in Release 08.0.90a.....	55
Closed with Code Changes in Release 08.0.90.....	60
Known Issues in Release 08.0.90a.....	90
Known Issues in Release 08.0.90.....	92

# Document History

Version	Summary of changes	Publication date
FastIron 08.0.90f for ICX Switches Version 1	Resolved issues	March 6, 2020
FastIron 08.0.90e for ICX Switches Version 1	Resolved issues	November 21, 2019
FastIron 08.0.90d for ICX Switches Version 1	Resolved issues	September 27, 2019
FastIron 08.0.90c for ICX Switches Version 2	FI-200763 and FI-200698 added to list of closed issues in FastIron 08.0.90c. Removed unrelated FastIron 08.0.91 issues.	August 30, 2019
FastIron 08.0.90c for ICX Switches Version 1	ICX devices now support fully qualified domain names for connection to SmartZone as described in <a href="#">New Software Features in 08.0.90c</a> on page 12.  Resolved issues.	August 29, 2019
FastIron 08.0.90b for ICX Switches Version 2	FI-201087 added to list of known issues in FastIron 08.0.90.	August 16, 2019
FastIron 08.0.90b for ICX Switches Version 1	SNMP behavior changed as described in <a href="#">New Software Features in 08.0.90b</a> on page 13.  Resolved issues.	May 28, 2019
FastIron 08.0.90a for ICX Switches Version 1	<ul style="list-style-type: none"> <li>Added LRM Adapter support for the ICX 7850</li> <li>Added MACsec support to the ICX 7850</li> <li>Resolved issues</li> </ul>	March 29, 2019
FastIron 08.0.90 for ICX Switches Version 3	Added resolved issue FI-194878 to Closed with Code Changes in 08.0.90.	February 26, 2019
FastIron 08.0.90 for ICX Switches Version 2	Correction to the list of new features	February 22, 2019
FastIron 08.0.90 for ICX Switches Version 1	New enhancements and features for the 08.0.90 release.	February 20, 2019



# Introduction

---

- [About FastIron Release 08.0.90](#)..... 7
- [Document Feedback](#)..... 7
- [Ruckus Product Documentation Resources](#)..... 7
- [Online Training Resources](#)..... 8
- [Contacting Ruckus Customer Services and Support](#)..... 8

## About FastIron Release 08.0.90

FastIron release 08.0.90 introduces the Ruckus ICX 7850 Switch, which delivers nonblocking line-rate performance on all ports concurrently, with a switching capacity up to 6.4 Tbps. It supports the next generation Ethernet speeds with 10/25 Gigabit Ethernet at the aggregation and 40/100 Gigabit Ethernet at the core to meet high volume of traffic driving from the edge into the core. The ICX 7850 also offers a range of features designed to simplify network deployment and management such as advanced stacking, and zero touch provisioning. Note that Bidirectional Forwarding, Campus Fabric, and VXLAN are not yet supported on the ICX 7850.

FastIron Release 8.0.90 introduces a number of key software features and enhancements to improve ICX switch management, usability, and scalability. New stacking features improve ease-of-use, including zero-touch provisioning, interactive setup, and stack unit location. New Layer 3 features include Bidirectional Forwarding Detection (on the ICX 7750 only) and IPv6 Neighbor Discovery (ND) Proxy. Other key management enhancements in FastIron 08.0.90 are SSH enabled out of the box and DHCPv6 server, which enables all ICX devices to be configured to function as DHCPv6 servers.

## 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](mailto:#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.

## Introduction

Online Training Resources

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

# Online Training Resources

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

# Contacting Ruckus Customer Services and Support

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

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

## What Support Do I Need?

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

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

## Open a Case

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

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

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

## Self-Service Resources

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

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>



- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—[https://support.ruckuswireless.com/#products\\_grid](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](https://support.ruckuswireless.com/case_management).



# New in This Release

---

• Hardware .....	11
• Important Changes in Release 08.0.90.....	12
• Software Features.....	12
• CLI Commands.....	15
• RFCs and Standards.....	20
• MIBs .....	20

## Hardware

The following section lists new hardware introduced with this release as well as hardware that is not supported with this release.

### Ruckus ICX 7850 Switch

#### Description

The new Ruckus ICX 7850 switch provides premium aggregation and core switching in which the network core layer can be distributed across the campus, deploying ports and switching capacity where they are needed.

The ICX 7850 48-port stackable aggregation switches come in 1/10 GbE and 1/10/25 GbE models. Both come standard with 8-ports of 40/100 GbE for stacking or uplinks. The 1/10 GbE model offers 48x 1/10 GbE ports with MACsec and LRM, the 1/10/25 GbE model offers 48x 1/10/25 GbE ports and 8x 40/100GbE ports for uplinks or stacking.

The ICX 7850-32Q aggregation/core switch comes standard with 32 40/100 GbE ports and up to 12 of these ports can be used for stacking. The QSFP28 ports are capable of native 40 GbE or 100 GbE Ethernet, or may be broken out to 4x10 Gbps or 4x25 Gbps links to give up to 128 10/25GbE ports for server aggregation in a Data Center, or switch aggregation in the campus.

#### Product Features

- Up to 32x 40/100 GbE ports per switch
- Up to 8x 100 GbE stacking ports, 1.6 Tbps of stacking bandwidth per switch
- Redundant, hot-swappable power supplies and fans
- In-Service Software Upgrades (ISSU)
- Multi-Chassis Trunking (MCT) for core failover with load-balancing
- Hitless stack insertion and removal
- Stacking scalability:
  - Up to 12 switches per stack
  - Up to 10 km using standard optics or cables
  - Up to 8x 40/100GbE standard QSFP28 stacking ports
- IPv4, IPv6, BGP, OSPF, VRRP, PIM, PBR, VRF
- Up to 48x 10/25GbE port per leaf switch for server connectivity
- Up to 32x 40/100 GbE ports per spine switch
- MACsec 128-bit and 256-bit data encryption

# Important Changes in Release 08.0.90

The following changes were introduced in FastIron Release 08.0.90:

- **Default Username and password:** New ICX switches that are initially deployed using the 08.0.90 release must be accessed using the following default local username and password:
  - Default local username: super
  - Default password: sp-adminThe default username and password apply to all forms of access including Console, SSH and WEB2. The administrator will be prompted to create a new password after logging in. ICX devices that are already deployed with a previous release and upgraded to 08.0.90 will not be affected by this change.
- **SSH enabled out of the box:** SSH is now enabled and Telnet is disabled by default on switches that do not have a startup-config file i.e. factory default configuration.
- **Software upgrade using a Unified FastIron Image (UFI) on the ICX 7850:** 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.
- **Non-UFI images do not support full functionality:** Note that the system does not support full functionality, such as third-party packages (DHCPv6, HTTP, Python, etc.,) without the UFI update.

Refer to the [Software Features](#) on page 12 section for a list of new features in this release. Refer to the FastIron Features and Standards Support Matrix, available at [www.ruckuswireless.com](http://www.ruckuswireless.com), for a detailed listing of feature and platform support.

## Software Features

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

### New Software Features in 08.0.90f

There are no new features in release 08.0.90f.

### New Software Features in 08.0.90e

There are no new features in release 08.0.90e.

### New Software Features in 08.0.90d

There are no new features in release 08.0.90d.

### New Software Features in 08.0.90c

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](http://www.ruckuswireless.com), for a detailed listing of feature and platform support.

Feature	Descriptions
FQDN for ICX-Management connection to SmartZone	An ICX device can receive a fully qualified domain name (FQDN) in response to a switch registrar query and use it to connect to ICX-Management on a SmartZone device. Previously, only IP addresses could be returned in response to a switch registrar query.

## New Software Features in 08.0.90b

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](http://www.ruckuswireless.com), for a detailed listing of feature and platform support.

Feature	Descriptions
Accessing RADIUS MIB objects through SNMP is enabled by default. As a result, a related command, <b>enable snmp config-radius</b> , has been deprecated.	Refer to the FastIron Security Configuration Guide for information on RADIUS or SNMP capabilities. Refer to the FastIron MIB Reference for information on MIB objects.
Accessing TACACS MIB objects through SNMP is enabled by default. As a result, a related command, <b>enable snmp config-tacacs</b> , has been deprecated.	Refer to the FastIron Security Configuration Guide for information on TACACS or SNMP capabilities. Refer to the FastIron MIB Reference for information on MIB objects.

## New Software Features in 08.0.90a

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](http://www.ruckuswireless.com), for a detailed listing of feature and platform support.

Feature	Descriptions
MACsec support on the ICX 7850	Refer to the FastIron Software Licensing Guide for information about getting a MACsec license for an ICX 7850.
LRM adapter module support on the ICX 7850	Ruckus ICX7150, ICX7250, ICX7750, and ICX 7850 Ethernet switches require a long-Reach Multimode (LRM) adaptor module to support LRM optics connections.

## New Software Features in 08.0.90

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](http://www.ruckuswireless.com), for a detailed listing of feature and platform support.

Feature	Descriptions
Software upgrade using a Unified FastIron Image (UFI) on the ICX 7850	A Unified FastIron Image (UFI), consisting of the application image, the boot code image, and the signature file, 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.
FastIron 08.0.90 support for the new ICX 7850 Switch	Nearly all FastIron features are supported on the ICX 7850, with the exception of Bidirectional Forwarding Detection, Campus Fabric, and OpenFlow. To see a detailed list of the specific features that are supported, refer to the FastIron Features and Standards Support Matrix, Release 08.0.90.

## New in This Release

### Software Features

Feature	Descriptions
Multiple VLAN Registration Protocol (MVRP)	MVRP is an IEEE 802.1ak Multiple Registration Protocol (MRP) application that allows dynamic VLAN configuration and distribution of VLAN membership information in a bridged local area network. An MVRP-aware switch can exchange VLAN configuration information with other MVRP-aware switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches. With MVRP, an access switch can be manually configured with all the desired VLANs for the network, and all other switches on the network can learn those VLANs dynamically. When the VLAN configurations on a switch are changed, MVRP automatically changes the VLAN configurations in the required switches.
LLDP on by default	The system enables the LLDP feature globally by default during boot up, for standalone switches and stacking mode. Applies only to new ICX switches from the factory or those that have been set back to the default configuration. Not supported in Campus Fabric implementations.
Default username and password	The device allows initial access only after using the default local username (super) and password (sp-admin). The administrator will be prompted to change the default password after logging in for the 1st time. ICX devices that are already deployed with a previous release and upgraded to 08.0.90 will not be affected by this change.
SSH enabled by default	This feature provides SSH access to the device out of the box, without the need for manual intervention to generate SSH keys.
LAG between different default port speeds	Config speed validation is performed as part of port addition to LAG, and ports with same config speed as that of the virtual LAG interface are accepted. This new feature adds validation of the duplex of the ports against the vlag interfaces in addition to the configuration speed validation.
MSTP path-cost configuration	This feature is enhanced to support MSTP in a range of ports.
TCP MSS	TCP MSS Adjustment feature is to avoid the overhead of fragmentation of the TCP data packet and to prevent TCP sessions getting time out due to non-support of fragmentation in the path.
Bidirectional Forwarding Detection (BFD)	BFD is a lightweight hello protocol, with little system overhead, used to rapidly detect link faults without overloading the system. BFD improves network performance by providing fast forwarding path failure detection times, switching traffic to an alternate path when necessary, in order to minimize traffic loss. BFD works by checking that the next-hop device is alive, thus providing rapid detection of the failure of a forwarding path. BFD can detect the failure of the forwarding plane in a sub-second time interval that is user-configurable. Supported on the ICX 7750 only.
Dynamic Host Configuration Protocol version 6 (DHCPv6) Server	DHCPv6 is a network protocol for configuring IPv6 hosts with IP addresses, IP prefixes, and other configuration data required to operate in an IPv6 network. All FastIron devices can be configured to function as DHCPv6 servers. DHCPv6 Server functions in the same manner as DHCP for IPv4, allocating temporary or permanent network IPv6 addresses to clients. DHCPv6 Server also allows for greater control of address distribution within a subnet.
Forwarding Profiles	Forwarding Profiles allows for the configuration of the Unified Forwarding Table (UFT) so that it suits deployment requirements. A predefined forwarding profile can be selected based on scaling requirements. This UFT partition is carried out during the initialization process and is effective after a system reload. Supported on the ICX 7850 only.
IPv6 Neighbor Discovery (ND) Proxy	IPv6 Neighbor Discovery(ND) Proxy enables the hosts in different broadcast domains or VLANs to communicate with each other. An IPv6 Proxy-enabled interface responds to a neighbor discovery request on behalf of host connected to another interface.
Syslog messages for xSTP	Syslog messages for xSTP inform if the CPU utilization is higher than the normal value and the BPDU processing rate is higher than the threshold limit. Syslog messages are generated depending upon the received STP or PVST BPDUs.

Feature	Descriptions
Packet Statistics Enhancement	This enhancement enables the system to count packets destined to the CPU based on programmable fields. The user can define the maximum unique field matches to be counted.
ICX 7850 stacking	Traditional stacks of up to 12 ICX 7850 units are supported
Interactive-setup for stacking replaces stack secure-setup	The stack interactive-setup command is introduced to streamline and assist in stack configuration. The stack secure-setup command is deprecated.
Zero-touch provisioning for stacking	The stack zero-touch-enable command is introduced to allow automatic stack configuration.
Elimination of required default-ports configuration	The default-ports command is deprecated beginning with this release. Configuring stacking ports is simplified.
Two-unit linear-topology stacking trunks	From this release, two-unit linear-topology trunks are supported on all ICX stackable models. The linear-topology trunk doubles the bandwidth of the stacking ports between two units and provides the same redundancy as a two-unit ring through trunk load balancing.
New configuration rules for stacking ports and trunks	Using the stack-port and stack-trunk commands is more intuitive, and some previous restrictions have been eliminated.

## CLI Commands

The commands listed in this section were introduced, modified, or deprecated in FastIron 08.0.90.

### New Commands in 08.0.90f

There are no new, modified, or deprecated commands in 08.0.90f.

### New Commands in 08.0.90e

There are no new, modified, or deprecated commands in 08.0.90e.

### New Commands in 08.0.90d

There are no new, modified, or deprecated commands in 08.0.90d.

### New Commands in 08.0.90c

There are no new, modified, or deprecated commands in 08.0.90c.

### New Commands in 08.0.90b

- **clear ipv6 dhcp6-server binding**
- **pool (DHCPv6)**

### Modified Commands in 08.0.90b

- **enable snmp**

## New in This Release

### CLI Commands

- **show ipv6 dhcp6-server**

## Deprecated Commands in 08.0.90b

- **enable snmp config-radius**
- **enable snmp config-tacacs**

## New Commands in 08.0.90a

No commands were introduced, modified, or deprecated in FastIron 08.0.90a.

## New Commands in 08.0.90

- **bfd**
- **bfd holdover-interval**
- **bfd min-tx**
- **bfd per-link**
- **clear mvrp**
- **clear pstat**
- **copy disk0 system-manifest**
- **dns-server (DHCPv6)**
- **domain-name (DHCPv6)**
- **enable-tcp-mss**
- **erase pre-8090-startup-backup**
- **forwarding-profile**
- **hmon client configuration**
- **hmon client statistics**
- **hmon client status**
- **hmon status**
- **ip ospf bfd**
- **ip route bfd**
- **ip route bfd holdover-interval**
- **ip tcp adjust-mss**
- **ipv6 dhcp6-server enable**
- **ipv6 multicast per-vlan filter-to-cpu**
- **ipv6 nd local-proxy**
- **ipv6 nd proxy**
- **ipv6 nd proxy-disable**
- **ipv6 ospf bfd**
- **ipv6 tcp adjust-mss**
- **linkdampen**



- **micro-bfd-enable**
- **name** (SPX, stacking)
- **neighbor bfd**
- **mvrp applicant-mode**
- **mvrp enable**
- **mvrp enable (Interface)**
- **mvrp point-to-point**
- **mvrp registration-mode**
- **mvrp timer**
- **mvrp vlan-creation-disable**
- **opaque-capability** (OSPFv2)
- **preferred-lifetime** (DHCPv6)
- **prefix6** (DHCPv6)
- **pstat**
- **pstat field-add**
- **pstat field-delete**
- **pstat max**
- **pstat save**
- **range6** (DHCPv6)
- **rapid-commit** (DHCPv6)
- **rebind-time** (DHCPv6)
- **refresh-time** (DHCPv6)
- **renewal-time** (DHCPv6)
- **show bfd**
- **show bfd agent**
- **show bfd applications**
- **show bfd counters**
- **show bfd ha info**
- **show bfd micro-session**
- **show bfd neighbors**
- **show bfd sessions**
- **show bfd trace session**
- **show bfd uc sessions**
- **show bfd v6-neighbors**
- **show bfd vrf**
- **show forwarding-profile**
- **show ip os-interface**
- **show ipv6 dhcp-server**
- **show mvrp**

## New in This Release

### CLI Commands

- **show pre-8090-startup-backup**
- **show pstat**
- **show pstat dump**
- **show pstat hist**
- **show pstat status**
- **show run mvrp**
- **show stack ipc stats**
- **show stack zero-touch ipc**
- **show stack zero-touch log**
- **show stack zero-touch status**
- **show sz sessions**
- **show sz tcp connections**
- **stack interactive-setup**
- **stack zero-touch-enable**
- **subnet6** (DHCPv6)
- **unit-name** (Stacking)
- **valid-lifetime** (DHCPv6)

## Modified Commands in 08.0.90

- **aaa authentication enable**
- **aaa authentication login**
- **aaa authentication snmp-server**
- **aaa authentication web-server**
- **clear macsec statistics**
- **copy tftp system-manifest**
- **default-ports**
- **dot1x-mka-enable**
- **enable egress-acl-on-cpu-traffic**
- **enable-mka**
- **errdisable recovery**
- **ip igmp max-group-address**
- **ip route**
- **ipv6 mld max-group-address**
- **key-server-priority**
- **macsec cipher-suite**
- **macsec confidentiality-offset**
- **macsec frame-validation**
- **macsec replay-protection**
- **mka-cfg-group**

- **pre-shared-key**
- **show cluster**
- **show default values**
- **show dot1x-mka config**
- **show dot1x-mka config-group**
- **show dot1x-mka sessions**
- **show dot1x-mka statistics**
- **show ip bgp neighbors**
- **show ip igmp traffic**
- **show ip interface**
- **show ip ospf config**
- **show ip ospf interface**
- **show ip tcp adjust-mss**
- **show ipv6 bgp neighbors**
- **show ipv6 interface**
- **show ipv6 mld traffic**
- **show ipv6 tcp adjust-mss**
- **show macsec statistics**
- **stack-port**
- **stack-trunk**
- **show vlan**

## Deprecated Commands in 08.0.90

- **authentication auth-default-vlan**
- **block-applicant**
- **block-learning**
- **clear gvrp statistics**
- **copy disk0 flash *file-name* bootrom**
- **copy disk0 flash *file-name* fips-bootrom-sig**
- **copy disk0 flash *file-name* fips-primary-sig**
- **copy disk0 flash *file-name* fips-secondary-sig**
- **copy tftp|scp flash *tftp server ip file -name* bootrom**
- **copy tftp|scp flash *tftp server ip file -name* fips-bootrom-sig**
- **copy tftp|scp flash *tftp server ip file -name* fips-primary-sig**
- **copy tftp|scp flash *tftp server ip file -name* fips-secondary-sig**
- **enable (GVRP)**
- **gvrp-base-vlan-id**
- **gvrp-enable**
- **gvrp-max-leaveall-timer**

## New in This Release

### RFCs and Standards

- **gvrp-timers**
- **join-timer leave-timer leaveall-timer**
- **auth-default-vlan**
- **default-ports** (stacking)
- **lldp run**
- **stack secure-setup**
- **show gvrp**
- **show gvrp ethernet**
- **show gvrp statistics**
- **show gvrp vlan**

## RFCs and Standards

The following RFCs and standards are newly supported in this release 08.0.90.

The following RFCs and standards are newly supported in this release.

- RFC 4087 IP Tunnel MIB
- RFC 5880 Bidirectional Forwarding Detection (BFD) -- Supporting asynchronous mode only
- RFC 5881 BFD for IPv4 and IPv6 (Single Hop)
- RFC 5883 BFD for Multi-Hop Paths
- RFC 7130 BFD on Link Aggregation Group (LAG) Interfaces
- IEEE 802.1ak Multiple Registration Protocol
  - Multiple MAC Registration Protocol (MMRP) is not supported.
  - Multiple VLAN Registration Protocol (MVRP) is supported in environments without spanning tree and environments with single spanning tree ONLY.
  - MVRP is not supported in environments with Per-VLAN spanning tree or multiple spanning tree.

## MIBs

The following sections list newly supported MIBs. See the Ruckus FastIron MIB Reference, Release 08.0.90 for details.

### New MIBs in Release 08.0.90

- RFC 4087 IP Tunnel MIB
- Stacking enhancements
- AAA authentication
- DHCP server

# Hardware Support

- Supported Devices ..... 21
- Technical Support Advisory..... 21
- Supported Power Supplies..... 22
- Supported Optics..... 22

## Supported Devices

The following devices are supported in release 08.0.90.

- ICX 7150 Series (ICX 7150-C12P, ICX 7150-24, ICX 7150-24P, ICX 7150-48, ICX 7150-48P, ICX 7150-48PF, ICX 7150-48ZP)
- ICX 7250 Series (ICX 7250-24, ICX 7250-24G, ICX 7250-24P, ICX 7250-48, ICX 7250-48P)
- ICX 7450 Series (ICX 7450-24, ICX 7450-24P, ICX 7450-32ZP, ICX 7450-48, ICX 7450-48F, ICX 7450-48P)
- ICX 7650 Series (ICX 7650-48P, ICX 7650-48ZP, ICX 7650-48F)
- ICX 7750 Series (ICX 7750-26Q, ICX 7750-48C, ICX 7750-48F)
- ICX 7850 Series (ICX 7850-32Q, ICX 7850-48FS, ICX 7850-48F)

## Technical Support Advisory

According to Technical Service Bulletin TSB-2019002-A, unexpected reboots --and, in some cases, hardware damage-- may occur due to a power-over-budget condition on some devices when a 10G-SFPP-TX-A transceiver is installed. Follow these instructions to avoid or correct the issue.

### Advisory Overview

**Affected Software Versions:** FI 08.0.90a and later releases

**Affected products:** ICX 7850-48F, ICX 7850-FS

**Symptoms:** Unexplained system reboot loop

**Summary:**

Copper transceiver 10G-SFPP-TX-A consumes more power than the normal 10-Gbps port with a typical SFP. The recommendations and restrictions in this section are provided to ensure safe operation of the transceiver. If you do not follow these recommendations, there is a risk of system instability and reboot. Damage to the circuit board and power supply may also occur.

**NOTE**

From Release FI 08.0.90c, when the transceiver is plugged in, a warning will appear advising what actions to take to avoid any power violation.

The following table describes ports that must be left open to avoid power violation.

**TABLE 1** Affected Hardware and Required Actions

ICX Model	10G-SFPP-TX-A Installed Location	Required Number of Unused SFP Ports for Each 10G-SFPP-TX-A installed
ICX 7850-48F/48FS	Built-in SFP ports	1

## Hardware Support

### Supported Power Supplies

**Corrective Action:** Cease using the 10G-SFPP-TX-A transceiver. Per the information provided in the previous table, leave the required number of SFP ports empty to remain within the allowable power budget before again using the transceiver.

## 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](http://www.ruckuswireless.com).

## Supported Optics

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

# Software Upgrade and Downgrade

- Image File Names..... 23
- PoE Firmware Files..... 23
- Open Source and Third Party Code..... 24

## Image File Names

Download the following images from [www.ruckuswireless.com](http://www.ruckuswireless.com).

Device	Boot image file name	Flash image file name	UFI file name (boot, image)
ICX 7150	mnz10115.bin	SPR08090f.bin/SPS08090f.bin	SPR08090fufi.bin/SPS08090fufi.bin
ICX 7250	spz101115.bin	SPR08090f.bin/SPS08090f.bin	SPR08090fufi.bin/SPS08090fufi.bin
ICX 7450	spz10115.bin	SPR08090f.bin/SPS08090f.bin	SPR08090fufi.bin/SPS08090fufi.bin
ICX 7650	tnu10115.bin	TNR08090f.bin/ TNS08090f.bin	TNR08090fufi.bin/TNS08090fufi.bin
ICX 7750	swz10115.bin	SWR08090f.bin/ SWS08090f.bin	SWR08090fufi.bin/SWS08090fufi.bin
ICX 7850	n/a	n/a	TNR08090fufi.bin

## PoE Firmware Files

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

Device	Firmware version	File name
ICX 7150	2.1.1 fw	icx7xxx_poe_02.1.1.b002.fw
ICX 7250	2.1.1 fw	icx7xxx_poe_02.1.1.b002.fw
ICX 7450	2.1.1 fw	icx7xxx_poe_02.1.1.b002.fw
ICX 7650	2.1.1 fw	icx7xxx_poe_02.1.1.b002.fw

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

**NOTE**

Please note the following recommendations and notices:

- Inline power is enabled by default as of FastIron release 08.0.70.
- As of FastIron release 08.0.70 **legacy-inline-power** configuration is disabled by default.
- Data link operation is decoupled from inline power by default as of FastIron release 08.0.70.
- Use the **[no] inline power** command to enable and disable POE on one or a range of ports.
- Data link operation is coupled with inline power using the command **inline power ethernet x/x/x couple-datalink** in Privileged EXEC mode or in interface configuration mode using the command **inline power couple-datalink**. The PoE behavior remains the same as in releases prior to 08.0.70 (08.0.30, 08.0.40, 08.0.50, 08.0.61).
- Do not downgrade PoE firmware from the factory installed version. When changing the PoE firmware, always check the current firmware version with the **show inline power detail** command, and make sure the firmware version you are installing is higher than the version currently running.
- The PoE microcontrollers are pre-programmed at the factory. The firmware can be loaded as an external file. The PoE firmware version string will be kept updated to match the corresponding FastIron software version; however, this is only a cosmetic change, and the firmware itself remains unchanged. If a new version of the code is released, Ruckus Technical Support will notify its customers of the needed code upgrade. Finally, in the remote case that a failure occurs during an upgrade process, the switch would still be functional but without PoE circuitry. If you encounter such an issue, please contact Ruckus Technical Support.
- PoE firmware will auto upgrade to version 2.1.0 fw during the loading of FastIron Release 08.0.80. This auto upgrade of the PoE firmware will add approximately 10 minutes to the loading of FastIron Release 08.0.80 on ICX 7150, ICX 7250, ICX 7450, and ICX 7650 devices.

## Open Source and Third Party Code

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

Manufacturer	Third Party Software
InMon	Sflow
Broadcom Inc	SDK 6.5.6
open source S/W	u-boot 2011.09
open source S/W	u-boot 2015.01
open source S/W	u-boot 2016.01
open source S/W	Linux OS: <ul style="list-style-type: none"> <li>• ICX7150, ICX7250, ICX7450: Linux 4.4</li> <li>• ICX7650, ICX7850: Linux 3.14.65</li> <li>• ICX7750: Linux 2.6.34.6</li> </ul>
Aquantia Inc	Aquantia phy driver AQR API 2.1.0
Aquantia	Aquantia phy drivers: <ul style="list-style-type: none"> <li>• ICX7150: AQR 3.5.E</li> <li>• ICX7450: AQR 2.C.5</li> <li>• ICX7650: AQR 3.5.E</li> <li>• ICX7750: AQR 1.38.11</li> </ul>
open source S/W	Parted utility
Broadcom Inc	Miura Phy driver 1.5



Manufacturer	Third Party Software
Broadcom Inc	EPDM driver 1.5.1
Spansion	Flash driver
<a href="http://www.bzip.org/">http://www.bzip.org/</a>	Bzip
<a href="http://www.hackersdelight.org/">http://www.hackersdelight.org/</a>	Integer square root computation
GNU ( <a href="http://www.gnu.org/">http://www.gnu.org/</a> )	LZMA SDK (compression method)
Freescale (NXP)	Software for PowerPC chip
Open Source SW	openssl_tpm_engine-0.4.2
Open Source SW	tpm-tools-1.3.8
Open Source SW	trousers-0.3.11.2
Infineon Technologies AG	ELTT_v1.3
Allegro Software	HTTP/HTTP-S, SSHv2
WindRiver	SNMPv1,v2c,v3; IPSecure
Interlink	Radius
SafeNet Sentinel RMS	Software Licensing Code - SafeNet Sentinel RMS
open source S/W	NSS 3.12.4 with NSPR 4.8
open source S/W	OpenSSL FIPS Object Module v2.0.5
open source S/W	OpenSSL crypto Ver 1.0.1e
GubuSoft	Javascript based tree display
GubuSoft	Javascript based tree display
GNU (The Regents of the University of California)	Syslog
BSD(The Regents of the University of California)	DNS Query/Resolution
BSD(The Regents of the University of California)	TimeZone Code (SNTP)
BSD(The Regents of the University of California)	Router Renumbering
BSD(The Regents of the University of California)	IPv6 defines
RouterWare Inc	TCP/IP stack, IPX, OSPFv2, TELNET, STP, LSL, TFTP client, BOOTP client and relay
IP Infusion	RIPng, OSPFv3, BGP4
open source S/W	libunwind
Wind River Systems, Inc.	Wind River MIB Compiler, version 10.2



# Issues

- Closed with Code Changes in Release 08.0.90f..... 27
- Closed with Code Changes in Release 08.0.90e..... 33
- Closed with Code Changes in Release 08.0.90d..... 36
- Closed with Code Changes in Release 08.0.90c..... 39
- Closed with Code Changes in Release 08.0.90b..... 51
- Closed with Code Changes in Release 08.0.90a..... 55
- Closed with Code Changes in Release 08.0.90..... 60
- Known Issues in Release 08.0.90a..... 90
- Known Issues in Release 08.0.90..... 92

## Closed with Code Changes in Release 08.0.90f

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.90f.

<b>Issue</b>	FI-208376
<b>Symptom</b>	Will not be able to configure BUM logging/port-dampening commands under multiple interface mode.
<b>Condition</b>	BUM logging/port-dampening commands under multiple interface mode
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

<b>Issue</b>	FI-208346
<b>Symptom</b>	Upgrade to 8090 release sometimes causes unexpected reload of the ICX device.
<b>Condition</b>	Upgrade to 8090 release
<b>Workaround</b>	The device comes up gracefully after the 2nd boot
<b>Recovery</b>	Automatically recovers after the 2nd boot
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - Software Installation and Upgrade

## Issues

Closed with Code Changes in Release 08.0.90f

<b>Issue</b>	FI-208289
<b>Symptom</b>	QSFP Links are not correctly detected and "show media" provides incorrect information.
<b>Condition</b>	1. Upgrade the ICX device to 8090 release and reload. 2. Another way to hit this problem is repeated fast plug-in and plug-out of QSFP
<b>Workaround</b>	NONE
<b>Recovery</b>	NONE
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	System - Optics

<b>Issue</b>	FI-208119
<b>Symptom</b>	"sh mem" displays high memory usage
<b>Condition</b>	Multiple iteration of snmpwalk to the ICX IF MIB creates memory leak
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - SNMP - Simple Network Management Protocol

<b>Issue</b>	FI-207928
<b>Symptom</b>	Unsupported CFM Trap is displayed in "sh snmp server" output.
<b>Condition</b>	Execute "sh snmp server"
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - SNMP - Simple Network Management Protocol

<b>Issue</b>	FI-207772
<b>Symptom</b>	After a reload there will be a mismatch between lag interface and member ports gig-default mode value, because of which lag becomes inactive.
<b>Condition</b>	Add ports which have GIG default mode configuration into the LAG. After a reload, LAG will be down.
<b>Workaround</b>	
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70 FI 08.0.90
<b>Technology / Technology Group</b>	System - CLI

<b>Issue</b>	FI-207596
<b>Symptom</b>	LG STB electronic devices loss connectivity with ICX devices.
<b>Condition</b>	When VLAN movement happens on MAC authentication, LG Set top boxes loss connectivity with ICX devices.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90 FI 08.0.91
<b>Technology / Technology Group</b>	Security - MAC Port-based Authentication

<b>Issue</b>	FI-206986
<b>Symptom</b>	SmartZone Config Backup does not work.
<b>Condition</b>	When 'telnet server enable vlan x' is configured, SZ config backup feature is not working.
<b>Workaround</b>	Remove the configuration, 'telnet server enable vlan x'.
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - Configuration Fundamentals

<b>Issue</b>	FI-206570
<b>Symptom</b>	Will experience excessive DHCP snooping syslog on DHCP snooping trusted port
<b>Condition</b>	Getting IP address from DHCP server will print this syslog Initiation of request for IP address from DHCP client to server will exchange many packets in the following order client to server ---- Discover server to client --- Offer client to server -- Request server to client - ACK When ACK is received on DHCP snooping trusted port this syslog will be logged
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Security

<b>Issue</b>	FI-197182
<b>Symptom</b>	Unexpected reload of ICX device when watchdog timeout occurred
<b>Condition</b>	When "sz disable" is issued, watchdog timeout occurred.
<b>Workaround</b>	None
<b>Recovery</b>	Switch will recover after reload
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - CLI - Command Line Interface

## Issues

Closed with Code Changes in Release 08.0.90f

<b>Issue</b>	FI-197299
<b>Symptom</b>	Reload of ICX device due to watchdog timeout.
<b>Condition</b>	many configurations pushed from SZ causing memory leak and then watchdog timeout
<b>Workaround</b>	None
<b>Recovery</b>	After reboot, switch will recover.
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management

<b>Issue</b>	FI-197848
<b>Symptom</b>	Unexpected reload of ICX device when watchdog timeout occurred
<b>Condition</b>	When "sz disable" is issued, watchdog timeout occurred.
<b>Workaround</b>	None
<b>Recovery</b>	Switch will recover after reload
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - CLI - Command Line Interface

<b>Issue</b>	FI-198600
<b>Symptom</b>	Unexpected reset during CPU control packet transmit operation
<b>Condition</b>	This can occur during a CPU control packet transmit
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-199245
<b>Symptom</b>	High CPU followed by watchdog timeout and crash will be observed in SPX CB units.
<b>Condition</b>	Issue happens only on CB units with large number of ports in default VLAN when STP is disabled in the default VLAN.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.91
<b>Technology / Technology Group</b>	Layer 2 Switching - VLAN - Virtual LAN

<b>Issue</b>	FI-202157
<b>Symptom</b>	After a prolonged period of SNMP MIB polls or CSL request handling (at least 8000 times or more) over SSH-reverse Tunnel, the ICX -switch may stop sending responses through the SNMP or HTTP channels of the SSH reverse Tunnel.
<b>Condition</b>	After a prolonged period of SNMP MIB polls or CSL request handling (at least 8000 times or more) over SSH-reverse Tunnel, the ICX -switch may stop sending responses through the SNMP or HTTP channels of the SSH reverse Tunnel.
<b>Workaround</b>	SZ disconnect or SZ disable and enable via CLI interface of ICX switch, is a way to recover when this issue happens.
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.92
<b>Technology / Technology Group</b>	Cloud Management

<b>Issue</b>	FI-206214
<b>Symptom</b>	SFLOW Counter samples does not have proper values and contain only zeros
<b>Condition</b>	Configure SFLOW in non-active unit interface and reload stack
<b>Workaround</b>	SFLOW disable and re-enable
<b>Recovery</b>	SFLOW disable and re-enable
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Monitoring - sFlow

<b>Issue</b>	FI-205255
<b>Symptom</b>	ICX device crash on bootup.
<b>Condition</b>	Device crash due to device certificate load. Issue happened due to fetching of non existent file from flash, which was due to incorrect file path used while opening the file
<b>Workaround</b>	NA
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - Software Installation and Upgrade

<b>Issue</b>	FI-204976
<b>Symptom</b>	After any configuration pushed from SZ, the originally "single-" option under config prompt gets replaced with per-VLAN STP options.
<b>Condition</b>	Any configuration pushed from SZ will trigger this issue.
<b>Workaround</b>	Save the configuration and then reload the system.
<b>Recovery</b>	Save the configuration and then reload the system.
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.90 FI 08.0.92
<b>Technology / Technology Group</b>	Layer 2 Switching - VLAN - Virtual LAN

## Issues

Closed with Code Changes in Release 08.0.90f

<b>Issue</b>	FI-204830
<b>Symptom</b>	SFLOW counter samples might not be received.
<b>Condition</b>	Configure SFLOW and reload the ICX device
<b>Workaround</b>	Disable and re-enable SFLOW
<b>Recovery</b>	Disable and re-enable SFLOW
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Monitoring - sFlow

<b>Issue</b>	FI-204805
<b>Symptom</b>	In ICX7150, the 2.5g port downshifts to 1g.
<b>Condition</b>	When ICX7150 is connected with R730 AP, the 2.5g port downshifts to 1g.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	System - System

<b>Issue</b>	FI-204445
<b>Symptom</b>	In ICX7650 with Rear module with 40G vs 100G, configured as uplink for stacking can have inconsistent message displays.
<b>Condition</b>	If the customer have ICX7650 with Rear modules of 100G speed operating in uplink mode and are planning to upgrade from FI8070 to FI8090 then they can see inconsistent messages when compared to 40G speed.
<b>Workaround</b>	Except the confirmation and proceed.
<b>Recovery</b>	Except the confirmation and proceed.
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90 FI 08.0.91 FI 08.0.92 FI 08.0.95
<b>Technology / Technology Group</b>	Stacking - Traditional Stacking

<b>Issue</b>	FI-203655
<b>Symptom</b>	Reserved VLAN 4094 are shown when ICX is managed through the web.
<b>Condition</b>	Configure web authentication and check the VLANs list in Web.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - SNMP - Simple Network Management Protocol



<b>Issue</b>	FI-203030
<b>Symptom</b>	Command to remove single-span config is not available. "no spanning-tree single"
<b>Condition</b>	When SZ tries to delete any of the port from 4094 vlan, "no spanning-tree single" is unavailable
<b>Workaround</b>	Reload the ICX device
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Layer 2 Switching - xSTP - Spanning Tree Protocols

<b>Issue</b>	FI-199642
<b>Symptom</b>	PoE power flap might be observed for some of the ports connected to POE device
<b>Condition</b>	When link is down on multiple ports and if PDs are not connected, POE port flaps will be experienced.
<b>Workaround</b>	Disable Non-PD detection using "no inline power non-pd-detection enable"
<b>Recovery</b>	Power recovers automatically.
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Management - PoE/PoE+ - Power over Ethernet

## Closed with Code Changes in Release 08.0.90e

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.90e.

<b>Issue</b>	FI-202279
<b>Symptom</b>	Unexpected reload will be observed when SZ disconnect command is invoked.
<b>Condition</b>	Invoke SZ disconnect command from console.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.91
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-203554
<b>Symptom</b>	ICX sends PIM Join/Prune messages with prefix set to 32 for IPv6 SSM group addresses.
<b>Condition</b>	When ICX device is configured with IPv6 SSM group addresses, it sends PIM Join/Prune messages with prefix set to 32 instead of 128. As a result, the client would not join/prune.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.91
<b>Technology / Technology Group</b>	

## Issues

Closed with Code Changes in Release 08.0.90e

Issue	FI-204085
Symptom	During stack switchover active unit system resets when we have uRPF and IPv6 static route with NULL0 nexthop interface configured.
Condition	When uRPF is enabled globally and IPv6 static route with NULL0 nexthop interface is configured, system reset is seen during stack switchover.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-198638
Symptom	In the ICX devices running with 8090x or later code, the memory leak might be seen when it is connected to SmartZone.
Condition	Memory leaks are seen when ICX is connected to SmartZone.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-203449
Symptom	The excessive DHCP Snooping SYSLOGs are seen.
Condition	Excessive logging when 'dhcp snooping client-learning disable' is configured.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

Issue	FI-204399
Symptom	The console login prompt overlaps with the longer MOTD message configured.
Condition	More than a page full of Message of the Day is configured, the login prompt gets overlapped.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

<b>Issue</b>	FI-203873
<b>Symptom</b>	Mcache entries are not created for SSM joins.
<b>Condition</b>	After reload, the mcache entries are not created for SSM joins.
<b>Workaround</b>	Removing and adding the command "ssm-enable range <acl-id>" solves the issue.
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.92
<b>Technology / Technology Group</b>	IP Multicast - PIM6 - IPv6 Protocol-Independent Multicast

<b>Issue</b>	FI-202630
<b>Symptom</b>	Adding support for Juniper's SPQ-CE-LR-CDFB-R1 100G LR4 support on Ruckus ICX switch
<b>Condition</b>	Adding support for Juniper's SPQ-CE-LR-CDFB-R1 100G LR4 support on Ruckus ICX switch
<b>Workaround</b>	NA
<b>Recovery</b>	NA
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-202303
<b>Symptom</b>	Occasionally ICX might unexpectedly reload while executing CLI "show snmp engineid".
<b>Condition</b>	1. When SNMP engine UP time is more than a day 2. Invoke CLI "show snmp engineid".
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - SNMP - Simple Network Management Protocol

<b>Issue</b>	FI-203359
<b>Symptom</b>	Password is displayed as plain text on configuring "password display"
<b>Condition</b>	"show ip bgp neigh" displays the password as plain text
<b>Workaround</b>	
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

## Issues

Closed with Code Changes in Release 08.0.90d

# Closed with Code Changes in Release 08.0.90d

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.90d.

Issue	FI-198548
<b>Symptom</b>	ICX device might experience NTP Synchronization error occasionally when the server is not reachable.
<b>Condition</b>	When there is NTP synchronization error and the ICX device is not able to recover by itself, invoke the new NTP reset CLI.
<b>Workaround</b>	Stack Switch-over
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Management - NTP - Network Time Protocol

Issue	FI-196102
<b>Symptom</b>	POE devices losing power during simulated redundant PS failure even though allocated power at failure is <740 watts
<b>Condition</b>	Have a redundant power source and make sure power drawn from ports. Make the redundant source to power down.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	

Issue	FI-200921
<b>Symptom</b>	One of the 7250-PE unit goes for unexpected reload on SPX
<b>Condition</b>	This symptom is seen while performing ISSU from 8090b to 8090c
<b>Workaround</b>	None
<b>Recovery</b>	Reload with desired Software image
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Stacking - Mixed Stacking

<b>Issue</b>	FI-201269
<b>Symptom</b>	Unexpected reload is seen when fitrace is issued through ssh
<b>Condition</b>	Invoke the below mentioned fitrace commands from a SSH session fitrace reset fitrace rate-limiting dis fitrace max unlimited fitrace destination terminal fitrace modules szagt_debug all level 1,2,3,4,5 fitrace modules ssh all level 1,2,3,4,5
<b>Workaround</b>	
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-201629
<b>Symptom</b>	Adding the second DC power supply causes the ICX device to reload.
<b>Condition</b>	When the ICX device is running with one DC power supply, inserting another DC or AC power supply causes the device to be reloaded.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-201881
<b>Symptom</b>	"Invalid port" error is thrown in the ICX device for a non-existent interface.
<b>Condition</b>	1. Configure sflow in an interface 2. Make the interface invalid by removing the corresponding module 3. write mem and re-load
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Management - sFlow

<b>Issue</b>	FI-201895
<b>Symptom</b>	Openflow command is accepted on LAG interface which is not supported.
<b>Condition</b>	Apply open flow command on LAG interface and it is accepted without any error.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

## Issues

Closed with Code Changes in Release 08.0.90d

<b>Issue</b>	FI-202004
<b>Symptom</b>	ICX7750 port LEDs do not light up when upgraded to 8090c.
<b>Condition</b>	This symptom is seen after the switch is upgraded to 8090c release.
<b>Workaround</b>	Switch can be downgraded to 8090b.
<b>Recovery</b>	Switch can be downgraded to 8090b.
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	System - Optics

<b>Issue</b>	FI-202035
<b>Symptom</b>	Unexpected reload of the ICX device is seen when nslookup command is invoked through SSH session.
<b>Condition</b>	1. Configure Ipv6 DNS server 2. Call nslookup from SSH Session
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90 FI 08.0.91
<b>Technology / Technology Group</b>	Layer 3 Routing/Network Layer - DNS - Domain Name System

<b>Issue</b>	FI-202215
<b>Symptom</b>	The interface configuration "ip ospf active" is not taking precedence over the global configuration "default-passive-interface".
<b>Condition</b>	If "default-passive-interface" is configured under "router ospf" after "ip ospf active" is configured on the interface, then the interface is incorrectly placed in the passive mode.
<b>Workaround</b>	Configure "no ip ospf active" followed by "ip ospf active" on the interface.
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Layer 3 Routing/Network Layer - OSPF - IPv4 Open Shortest Path First

## Closed with Code Changes in Release 08.0.90c

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.90c.

<b>Issue</b>	<b>FI-200763</b>
Symptom	ICX does not re-authenticate the clients under certain rare conditions.
Condition	When the MAC address moves from port to port, MAC authentication also needs to be re-tried.
Workaround	None.
Recovery	Issue 'clear auth session' to trigger the re-authentication.
Probability	Medium
Found In	FI 08.0.90
Technology/ Technology Group	Security - MAC Port-based Authentication

<b>Issue</b>	<b>FI-200759</b>
Symptom	DHCP packets are dropped at the ICX which operate as DHCP-Relay
Condition	DHCP-Relay and DHCP-Server are enabled in ICX with no address pool configuration.
Workaround	If there are no address-pool, the DHCP-Server configuration can be removed.
Recovery	
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	

<b>Issue</b>	<b>FI-200698</b>
Symptom	A stack can see two Active switches under certain conditions.
Condition	When an active unit resets, the standby unit takes over and becomes the new active controller. The old active comes back as an active controller, but it will be reset by the new active controller to come up as a member. (A stack system can have only one active controller.) The problem is that it takes more than one minute for the new active controller to reset the old active controller. The data ports of the old unit have come up. Then other devices that has link aggregation (LAG) to the ports of both units will messed up because the old unit will soon be reloaded.
Workaround	The issue eventually recovers after the old active controller is reloaded again. However, this cause traffic interruption for the transit period.
Recovery	None
Probability	Low
Found In	FI 08.0.80 FI 08.0.90 FI 08.0.91
Technology/ Technology Group	Stacking - Stack Management

## Issues

Closed with Code Changes in Release 08.0.90c

<b>Issue</b>	<b>FI-201109</b>
Symptom	The phone session gets cleared around every minute with the error message "[Termination-cause: Phone-Toggle]".
Condition	Phone session is constantly cleared with Mac-filter override for 802.1x port is configured.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70 FI 08.0.90
Technology/ Technology Group	Security - 802.1x Port-based Authentication

<b>Issue</b>	<b>FI-201171</b>
Symptom	ICX devices running as CB unit in SPX setup goes for unexpected reload.
Condition	When the ACL filter is modified/duplicated, ICX devices running as CB unit in SPX setup goes for unexpected reload.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	Security - ACLs - Access Control Lists

<b>Issue</b>	<b>FI-200719</b>
Symptom	OSPF adjacency will not form when MD5 authentication and KEYCHAIN is enabled.
Condition	Configure KEYCHAIN and MD5 authentication. Ospf adjacency will fail.
Workaround	
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology/ Technology Group	Layer 3 Routing/Network Layer - OSPF - IPv4 Open Shortest Path First



<b>Issue</b>	<b>FI-199095</b>
Symptom	After "stack switchover", if "enable" typed on new-active console within 10 seconds, then first time config/unconfig/clear doesn't sync to standby, all clis throw error
Condition	enter CLI commands enable commands immediately after the switchover command.
Workaround	Wait for more than 10 sec or more before enter any commands after switchover.
Recovery	Wait for more than 10 sec or more before enter any commands after switchover.
Probability	
Found In	FI 08.0.91
Technology/ Technology Group	Stacking - Traditional Stacking

<b>Issue</b>	<b>FI-200698</b>
Symptom	When an active unit resets, the standby unit takes over and becomes the new active controller. The old active comes back as an active controller, but it will be reset by the new active controller to come up as a member. (A stack system can have only one active controller.) The problem is that it takes more than one minute for the new active controller to reset the old active controller. The data ports of the old unit have come up. Then other devices that has link aggregation (LAG) to the ports of both units will messed up because the old unit will soon be reloaded.
Condition	publish because this is a customer issue.
Workaround	The issue eventually recovers after the old active controller is reloaded again. However, this cause traffic interruption for the transit period.
Recovery	None
Probability	High
Found In	FI 08.0.80 FI 08.0.90 FI 08.0.91
Technology/ Technology Group	

<b>Issue</b>	<b>FI-200553</b>
Symptom	IGMP join messages that are initiated by the client are not reflected in the IGMP tables.
Condition	When the client application is leaving a group and joining another group and if it is sending IGMP join messages that are initiated by the client (not as a response to a query) are not reflected in the IGMP tables.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology/ Technology Group	IP Multicast - IGMP - Internet Group Management Protocol

## Issues

Closed with Code Changes in Release 08.0.90c

<b>Issue</b>	<b>FI-196017</b>
Symptom	In ICX7450, the link fault signalling is not working in 10G port.
Condition	When ICX7450 devices are connected through 10G ports, if Rx cable of one of the devices is removed, the other side port status is still shown as Up though link fault signalling is configured.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70 FI 08.0.80
Technology/ Technology Group	System - Optics

<b>Issue</b>	<b>FI-200346</b>
Symptom	The next-bootstrap-server option config is not allowed.
Condition	When configuring the next-bootstrap-server feature, the error "Error: Configured option <54> is default/unsupported" is thrown.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology/ Technology Group	

<b>Issue</b>	<b>FI-200299</b>
Symptom	UDP ports 2068 to 2090 are seen as OPEN when connected via console/ telnet/ssh
Condition	When scanning for UDP ports using tools like netcat, the ports 2068 to 2090 are seen as OPEN when connected via Console/Telnet/SSH
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	Cloud Management - DNS

<b>Issue</b>	<b>FI-198207</b>
Symptom	ICX DHCPv6 server not assigning ipv6 address to the client when running with Switch image.
Condition	When stack MAC other than Active unit's MAC is configured in ICX DHCPv6 server running with switch image, the clients are assigned with IPv6 address.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	Management - DHCP (IPv6)

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

## Issues

Closed with Code Changes in Release 08.0.90c

<b>Issue</b>	<b>FI-199067</b>
Symptom	Stack unit might reload when ping to VRRP IP address.
Condition	Ping to VRRP IP address.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.70
Technology/ Technology Group	Other - Other

<b>Issue</b>	<b>FI-194518</b>
Symptom	The system hangs and the watchdog timeout happens to reload the device.
Condition	This is due to the HW ECC error on the NAND device. This can occur at random.
Workaround	There is no workaround.
Recovery	The device should be automatically recovered with the watchdog timer.
Probability	Low
Found In	FI 08.0.90 FI 08.0.91
Technology/ Technology Group	System - System

<b>Issue</b>	<b>FI-198474</b>
Symptom	Port utilization Receive and Transmit Peak values are displayed more than 100% while checking through web-management.
Condition	Device statistics are read by accessing the device through web-management.
Workaround	-
Recovery	-
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	Management - Web Management

<b>Issue</b>	<b>FI-198880</b>
Symptom	Junk value in Mac-Authentication SNMP Traps.
Condition	When the Mac-Authentication interface is from non-active units.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.70
Technology/ Technology Group	

<b>Issue</b>	<b>FI-198736</b>
Symptom	Some license files or configuration files are missing after the filesystem corruption happens.
Condition	This occurs when the filesystem is corrupted and the system is recovered.
Workaround	There is no workaround.
Recovery	Re-installing the missing license files and re-creating the startup configuration.
Probability	Low
Found In	FI 08.0.70 FI 08.0.61 FI 08.0.80 FI 08.0.90 FI 08.0.91
Technology/ Technology Group	System - System

<b>Issue</b>	<b>FI-198729</b>
Symptom	Some daemon processes (some applications running at background for services) are not stopped automatically at shutdown.
Condition	This occurs every time the device reloads.
Workaround	There is no workaround.
Recovery	The system forcefully stop those processes (applications) to reload in the end.
Probability	High
Found In	FI 08.0.90 FI 08.0.91
Technology/ Technology Group	System - System

## Issues

Closed with Code Changes in Release 08.0.90c

<b>Issue</b>	<b>FI-198353</b>
Symptom	Multicast Packets are not being learnt
Condition	Multicast Packets are not being learnt when PE port is moved from being a tagged port in user VLAN to an untagged port in default VLAN
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90 FI 08.0.91
Technology/ Technology Group	Layer 2 Switching - QnQ - IEEE 802.1Q

<b>Issue</b>	<b>FI-198247</b>
Symptom	Image copy might fail to PE via USB UFI upgrade.
Condition	ICX software image copy happens via USB when 1Cb-1PE topology is configured.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.90
Technology/ Technology Group	System - System

<b>Issue</b>	<b>FI-198240</b>
Symptom	If a user VRF is deleted, when IPv6 PIM sparse is enabled on interface belonging to that VRF, system may crash under certain conditions later when some other configuration is done on those interface.
Condition	System may crash in the following conditions 1. A user VRF is configured with IPv6 PIM sparse enabled on interface belonging to that user VRF. 2. That user VRF is deleted without removing "ipv6 router pim vrf <>" configuration for that user VRF or without removing "ipv6 pim-sparse" configuration on the interfaces belonging to that VRF. 3. As the user VRF is deleted, those interfaces will now will be moved to default VRF. 4. If one of those interfaces is deleted or if "ipv6 pim-sparse" configuration is done on one of those interfaces, system may crash.
Workaround	Before deleting user VRF, remove the "ipv6 router pim vrf <>" configuration for that user VRF.
Recovery	
Probability	
Found In	FI 08.0.90 FI 08.0.91
Technology/ Technology Group	

<b>Issue</b>	<b>FI-198022</b>
Symptom	Web access to ICX allow configuring invalid module.
Condition	Web access to ICX and trying to configure invalid module
Workaround	-
Recovery	
Probability	
Found In	FI 08.0.90 FI 08.0.91
Technology/ Technology Group	

<b>Issue</b>	<b>FI-197864</b>
Symptom	This issue can be caused by the UBIFS errors and re-formatting as follows. UBIFS error (ubi0:0 pid 566): ubifs_recover_leb: corrupt empty space LEB 3:12288, corruption starts at 1009713 UBIFS error (ubi0:0 pid 566): ubifs_scanned_corruption: corruption at LEB 3:1022001 UBIFS error (ubi0:0 pid 566): ubifs_scanned_corruption: first 8192 bytes from LEB 3:1022001 UBIFS error (ubi0:0 pid 566): ubifs_recover_leb: LEB 3 scanning failed mount: mounting ubi0:config on /fast_iron failed: Structure needs cleaning Mounting Config partition failed, non-recoverable file system corruption Reformatting the flash, please download config and keys again ... Formatting Done
Condition	This is a NAND flash HW (ECC) error, and this can occur at random at boot.
Workaround	There is no workaround.
Recovery	
Probability	
Found In	FI 08.0.60
Technology/ Technology Group	System - System

<b>Issue</b>	<b>FI-196178</b>
Symptom	ICX7850 standalone device operating in uplink-40g mode shows 1/3/3 as stack-port in the configuration.
Condition	When ICX7850 standalone device operates in uplink-40g mode, doing "write memory" adds 1/3/3 as stack-port in the configuration.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	Stacking - Stack Management

## Issues

Closed with Code Changes in Release 08.0.90c

<b>Issue</b>	<b>FI-196569</b>
Symptom	Core dump is generated on configuring/ un-configuring LAG
Condition	Configure/un-configure LAG interface.
Workaround	
Recovery	None
Probability	Low
Found In	FI 08.0.70
Technology/ Technology Group	Layer 2 - Link Aggregation

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

<b>Issue</b>	<b>FI-197207</b>
Symptom	The configuration "authentication auth-filter" is corrupted or lost.
Condition	When "authentication auth-filter" is configured on the interface, the configuration is getting corrupted and also lost if reloaded.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.91
Technology/ Technology Group	Management - CLI - Command Line Interface



<b>Issue</b>	<b>FI-195514</b>
Symptom	ACL applied on physical interfaces/virtual interface will not block all UPnP packets.
Condition	ACL is applied to block UPnP packets.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.80
Technology/ Technology Group	Security - ACLs - Access Control Lists

<b>Issue</b>	<b>FI-196253</b>
Symptom	SNMP/HTTP channel specific syslog messages are overwriting the actual SZ (Smart Zone) connection error logs in "show sz log" output.
Condition	Syslogs are getting overwritten when syslog is enabled for SZ module.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.90
Technology/ Technology Group	Management - SSH2 & SCP - Secure Shell & Copy

<b>Issue</b>	<b>FI-196335</b>
Symptom	No Syslog generated when radius-server/client key updated.
Condition	When Radius-server/Client key updated.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	

## Issues

Closed with Code Changes in Release 08.0.90c

<b>Issue</b>	<b>FI-196262</b>
Symptom	Device reboots silently without any warning message due to high CPU temperature.
Condition	Device reboots silently without any warning message due to high CPU temperature.
Workaround	Should maintain the optimal temperature so that device temperature won't go for very high values.
Recovery	Since device go for reboot, it will automatically boots up.
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	

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

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

<b>Issue</b>	<b>FI-194818</b>
Symptom	'show pdc data-ready-units' commands retains the data availability information even when the PE unit is detached.
Condition	PDC is enabled. The PE unit had PDC data and got detached.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	Other - Other

<b>Issue</b>	<b>FI-194812</b>
Symptom	When pdc data transfer tftp is configured and reloaded the config doesnt persist
Condition	pdc data transfer tftp configured Reload
Workaround	After reload pdc data transfer tftp can be reconfigured
Recovery	pdc data transfer can be configured manually
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	Other - Other

## Closed with Code Changes in Release 08.0.90b

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.90b.

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

## Issues

Closed with Code Changes in Release 08.0.90b

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

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

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

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

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

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

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

<b>Issue</b>	FI-196466
<b>Symptom</b>	Private VLAN port is allowed to be configured in a regular VLAN and vice versa with the following message. "Warning: port <x> in Private VLAN is added to Regular VLAN <y> as Tagged Member.
<b>Condition</b>	Customer should have PVLAN and regular VLAN configured.
<b>Workaround</b>	N/A
<b>Recovery</b>	N/A
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Security

## Issues

Closed with Code Changes in Release 08.0.90b

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

<b>Issue</b>	FI-196472
<b>Symptom</b>	Sflow data showing default VLAN ID instead of VLAN where user is placed.
<b>Condition</b>	Sflow data shows incorrect VLAN ID in the standby unit, when the host on the port is mac-authenticated.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

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

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

## Closed with Code Changes in Release 08.0.90a

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.90a.

<b>Issue</b>	FI-184047
<b>Symptom</b>	System crash while freeing the mac entry.
<b>Condition</b>	System configured with overlay-gateway configuration. And LAG is part of VNI mapped VLAN and some MACs are on that LAG interface. And then while deleting the LAG interface, user may see the crash.
<b>Workaround</b>	Before deleting the LAG interface, perform "clear mac" on LAG interface and then delete LAG interface.
<b>Recovery</b>	Reload the system.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	

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

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

## Issues

Closed with Code Changes in Release 08.0.90a

Issue	FI-195702
<b>Symptom</b>	"show ipv6 dhcp6-server lease" command does not reflect all the leases that have been issued by the DHCPv6 server running on ICX. Only some or none of the leases may be shown. Also, when an existing lease information expires for a device, it might be assigned a different IP (as opposed to the IP it is trying to renew)
<b>Condition</b>	This issue will be seen in ICX 7K devices running FI 08.0.90 after the device reloads (in stand-alone devices) or after switchover/failover (in stacking topologies)
<b>Workaround</b>	None
<b>Recovery</b>	No manual recovery is operationally necessary. Even though the lease information stored by the DHCPv6 server is not complete, it will not assign the same IP to multiple devices. During address assignment, before assigning an IP, the server will ensure that no other device it has serviced is using the IP it is going to assign to a new device.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

Issue	FI-194591
<b>Symptom</b>	When SmartZone is reachable through a management-vrf, ICX is not able to establish a session with SmartZone. SmartZone will be unable to monitor the ICX device. The following Syslog will be seen on the ICX when trying to connect to SmartZone - Feb 12 10:55:46:!:SZAgent: SZ Query to <SZ-IP> Failed. Reason: HTTPS Connection Error
<b>Condition</b>	Seen in images FI 08.0.80 and above, when SmartZone is reachable through the management-vrf and management-vrf is configured similar to the example below - interface management 1 vrf forwarding test no ip dhcp-client enable ip address <IP> <SubnetMask> !
<b>Workaround</b>	NA
<b>Recovery</b>	NA
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	

Issue	FI-193353
<b>Symptom</b>	IPv6 Route table full and IPv4 route table Full error messages would be printed in console.
<b>Condition</b>	1. Configure reverse-path-check. 2. Ping or tcp/udp scan an IPv6 subnet on ICX7K device to add more than 1024 IPv6 routes.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70 FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	



<b>Issue</b>	FI-194347
<b>Symptom</b>	Sensors connected to ICX on 10Gb port stops working after a period of time.
<b>Condition</b>	When sensors are connected to ICX on 10Gb port, they stop working due to autonegotiation issue with 100M after a period of time.
<b>Workaround</b>	Disable and enable the port recovers this issue.
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	System - System

<b>Issue</b>	FI-193916
<b>Symptom</b>	On ICX device, ssh session hangs sometimes without displaying prompt.
<b>Condition</b>	Sometimes ssh login might hang after the initial password entry.
<b>Workaround</b>	Retry the ssh login, and it'll succeed.
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	Management - SSH2 & SCP - Secure Shell & Copy

<b>Issue</b>	FI-194208
<b>Symptom</b>	ICX7750-48F 10/40 Gbps LED stays as steady green.
<b>Condition</b>	When traffic is passing through ICX7750-48F, 10/40 Gbps LED stays as steady green instead of blinking.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-193199
<b>Symptom</b>	Removing a sequence from a ACL and reapplying doesn't work as expected.
<b>Condition</b>	Issue is seen only when ACL has multiple sequences. The sequence which is removed and re-added should be before a deny rule for the issue to occur.
<b>Workaround</b>	Remove and re-add entire ACL resolve's the issue.
<b>Recovery</b>	Remove and re-add entire ACL recover's the issue.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

## Issues

Closed with Code Changes in Release 08.0.90a

<b>Issue</b>	FI-192861
<b>Symptom</b>	ICX7850-48FS may show a series of IDM fault message like "[ 8983.951661] iproc-idm idm: idm_pcie_0_ds11 ( 5 21009900 367) fault" and LED behavior may be affected. On rare conditions system might reload to recover.
<b>Condition</b>	When used with macsec traffic in ICX7850-48FS, system may show a series of IDM fault message like "[ 8983.951661] iproc-idm idm: idm_pcie_0_ds11 ( 5 21009900 367) fault" and LED behavior may be affected. On rare conditions system might reload to recover.
<b>Workaround</b>	Not configuring MACSEC in ICX7850-48FS can prevent this issue.
<b>Recovery</b>	system might automatically reload to recover.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-191652
<b>Symptom</b>	Crash is seen when IPV6 client is trying to get an IP address from dhcpv6 server with dhcpv6 snooping enabled.
<b>Condition</b>	Issue is seen only when Dhcpv6 snooping is enabled and client is getting IP address from the server .
<b>Workaround</b>	N/A
<b>Recovery</b>	N/A
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70 FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-102190
<b>Symptom</b>	High CPU utilization due to UDP traffic destined for port 520 forwarded to CPU.
<b>Condition</b>	UDP traffic with destination port as 520.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Layer 3 Routing/Network Layer - RIP - IPv4 Routing Information Protocol

<b>Issue</b>	FI-190488
<b>Symptom</b>	Though 40GE-Active Copper 1m (QSFP+) is supported, show media eth x/x/x showed it as unsupported. No impact on functionality
<b>Condition</b>	show media eth x/x/x displays that the 40GE-Active Copper 1m (QSFP+) is not supported.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	System - Optics

<b>Issue</b>	FI-190426
<b>Symptom</b>	As part of PDC framework, added additional CLI command support for PDC Custom Command and Event history.
<b>Condition</b>	Added additional CLI command support for PDC Custom Command and Event history.
<b>Workaround</b>	Nil.
<b>Recovery</b>	Nil.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-190220
<b>Symptom</b>	Mac address table will not get updated when ports move from one vlan to another on single span environment. This will result in stale mac entries.
<b>Condition</b>	Enable single span. Add ports under one Vlan. On receiving traffic in those ports, the mac entries will get added with corresponding Vlan id. Move the ports to another Vlan . Now the previous mac entries learned through the old Vlan should get deleted and new mac entries should get added with the current Vlan id . But in issue state,mac address learned through old Vlan will not be removed / updated and will get deleted only on time out.
<b>Workaround</b>	NA
<b>Recovery</b>	NA
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Layer 2 Switching - VLAN - Virtual LAN

<b>Issue</b>	FI-188610
<b>Symptom</b>	Switch may reload if BUM rate limits are configured on all ports of the switch/stack.
<b>Condition</b>	BUM rate limiting is configured on all ports of the respective unit
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

<b>Issue</b>	FI-187692
<b>Symptom</b>	On snmp walk , ifNumber object would display wrong value
<b>Condition</b>	1. Configure snmp server 2. Do snmp walk for the object IF-MIB::ifNumber.0 3. On snmp walk , ifNumber object would display wrong value
<b>Workaround</b>	NA
<b>Recovery</b>	NA
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Management - SNMP - Simple Network Management Protocol

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-188315
<b>Symptom</b>	When supportsave is issued more than once and if the first supportsave fails core file will get deleted.
<b>Condition</b>	1. Issue supportsave command to collect the core file. 2. GZIP fails to compress the file. 3. Core file is removed even when the supportsave fails. 4. Core file cannot be recovered by subsequent supportsave command.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Management - Configuration Fundamentals

<b>Issue</b>	FI-187565
<b>Symptom</b>	When all the ports in lag is removed, the ICX device reloads spontaneously.
<b>Condition</b>	LAG is configured on an ICX device and all the ports in lag are removed.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	Layer 2 Switching - LAG - Link Aggregation Group

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

## Closed with Code Changes in Release 08.0.90

This section lists software issues with Critical, High, and Medium Technical Severity closed with a code change in release 08.0.90.

<b>Issue</b>	FI-194878
<b>Symptom</b>	ICX device does not get dynamic IP address assigned, when acting as DHCP Client.
<b>Condition</b>	When UBEE cable modem is configured as DHCP Server, the ICX DHCP client does not get IP address assigned.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-193990
<b>Symptom</b>	The ICX device reloads unexpectedly.
<b>Condition</b>	The ICX device reloads due to OSPF, when more LSAs are received and if there is any flapping with external LSAs.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-193938
<b>Symptom</b>	System may become unstable when a large list of ports are configured under a VLAN.
<b>Condition</b>	When a 'scaled' CLI with large number of ports - reaching the limits of the CLI buffer - is configured under a VLAN, system becomes unstable.
<b>Workaround</b>	Limiting only a few ports to a VLAN.
<b>Recovery</b>	Recover the switch with factory default configuration.
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.70 FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	Management - CLI - Command Line Interface

<b>Issue</b>	FI-192173
<b>Symptom</b>	IP-ACL does not block Multicast Traffic
<b>Condition</b>	Incoming Traffic which has Multicast IP Address as Source Address is not blocked by IP-ACL
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

<b>Issue</b>	FI-193003
<b>Symptom</b>	Following error printed on console and cli did not work. Reload of the device resolved the issue. "unit 0: Retry DEFIP AUX Operation.. unit 0: DEFIP AUX Operation encountered parity error !! Mem: Unit 0: mem: 2067=L3_DEFIP_DATA_ONLY blkoffset:10 Unit 0: CLEAR_RESTORE: L3_DEFIP_PAIR_128_DATA_ONLY[2073] blk: ipipe0 index: 287 : [1][28480000] "
<b>Condition</b>	NA
<b>Workaround</b>	Reload of the switch resolved the error and cli worked fine after reload.
<b>Recovery</b>	NA
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	System - System

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-193462
<b>Symptom</b>	user may sometimes see an error message in the console like below "I2C_CORE: B80:D51 Read Failed.Bytes read=0 Bytes to read=1"
<b>Condition</b>	under rare circumstances user might see an i2c error in the console of ICX7650. This has no functional impact on the switching and routing capability of the device.
<b>Workaround</b>	No workaround available.
<b>Recovery</b>	No recovery needed. It automatically recovers
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-192266
<b>Symptom</b>	Feature support to forward UDP flows to a sub-net broadcast address.
<b>Condition</b>	Feature support to forward UDP flows to a sub-net broadcast address.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Layer 3 Routing/Network Layer - IP Addressing

<b>Issue</b>	FI-193357
<b>Symptom</b>	Port Link doesn't come up when connected to multi gig ports of 7150-48ZP.
<b>Condition</b>	Devices connected On Multi-gig ports of 7150-48ZP doesn't come up due to auto negotiation failure .
<b>Workaround</b>	Configure 1000-full-slave on the ICX as a workaround
<b>Recovery</b>	N/A
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - PoE/PoE+ - Power over Ethernet

<b>Issue</b>	FI-192861
<b>Symptom</b>	ICX7850-48FS may show a series of IDM fault message like "[ 8983.951661] iproc-idm idm: idm_pcie_0_ds11 ( 5 21009900 367) fault" and LED behavior may be affected. On rare conditions system might reload to recover.
<b>Condition</b>	When used with macsec traffic in ICX7850-48FS, system may show a series of IDM fault message like "[ 8983.951661] iproc-idm idm: idm_pcie_0_ds11 ( 5 21009900 367) fault" and LED behavior may be affected. On rare conditions system might reload to recover.
<b>Workaround</b>	Not configuring MACSEC in ICX7850-48FS can prevent this issue.
<b>Recovery</b>	system might automatically reload to recover.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-190996
<b>Symptom</b>	On a ICX 7650-48f stack, the standby/member deleted itself from the stack and then reloaded. After reboot the module gets stuck in continues boot loop.
<b>Condition</b>	On a ICX7650-48f stack, when configure "speed-duplex 1000-full" in interface range mode for standby/member, the module struck for some time and then reloaded.
<b>Workaround</b>	Configure the "speed-duplex 1000-full" in a smaller range of interfaces.
<b>Recovery</b>	Remove "speed-duplex 1000-full" configuration in standby/member and Configure the "speed-duplex 1000-full" in a smaller range of interfaces.
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.70 FI 08.0.90
<b>Technology / Technology Group</b>	System - System

<b>Issue</b>	FI-192117
<b>Symptom</b>	Code upgrade from SZ fails when 'enable telnet authentication' and TACACS+ are used together.
<b>Condition</b>	The issue is seen only when 'enable telnet authentication' and TACACS+ are used together.
<b>Workaround</b>	None
<b>Recovery</b>	Disable telnet authentication as a workaround
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	Cloud Management - Switch Registrar/Tunnel Aggregator

<b>Issue</b>	FI-191512
<b>Symptom</b>	While running power line disturbance tests, the SSH host key stored on the flash is lost
<b>Condition</b>	SSH key files may get lost when 1) Power Line Disturbance tests are run 2) EEC errors occur in the flash partition 3) Erasing of the flash partition 4) UBI file system corruption
<b>Workaround</b>	NA
<b>Recovery</b>	Re-generate SSH key files
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.61 FI 08.0.90
<b>Technology / Technology Group</b>	Management - SSH2 and SCP - Secure Shell and Copy

<b>Issue</b>	FI-192003
<b>Symptom</b>	A switch may get into rolling reloads if a very large port list is configured to a VLAN, save that configuration and execute reload command.
<b>Condition</b>	This issue happens when a large number of ports are configured to a VLAN, save the running-config to startup config and reload the switch.
<b>Workaround</b>	When configuring the ports, using 'to' keyword would prevent the issue from happening.
<b>Recovery</b>	
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Layer 2 Switching - VLAN - Virtual LAN

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-102190
<b>Symptom</b>	High CPU utilization due to UDP traffic destined for port 520 forwarded to CPU.
<b>Condition</b>	UDP traffic with destination port as 520.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Layer 3 Routing/Network Layer - RIP - IPv4 Routing Information Protocol

<b>Issue</b>	FI-191216
<b>Symptom</b>	Traffic dropped by Default Null Route despite better eBGP Default Route
<b>Condition</b>	When configuring a Default Null Route with higher admin distance than the Default Route received by eBGP, after reload traffic is getting dropped. When unconfiguring the default Null Route , the traffic is still not resumed.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Layer 3 Routing/Network Layer - BGP4 - IPv4 Border Gateway Protocol

<b>Issue</b>	FI-190837
<b>Symptom</b>	some of the ports will not power PDs and "show inline power" shows different ports as powered while the PDs are connected on some other ports.
<b>Condition</b>	one or more PoE HWs are sensing voltage drift. This HW may or may not recover.
<b>Workaround</b>	move to 8070d
<b>Recovery</b>	move to 8070d
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.70 FI 08.0.90
<b>Technology / Technology Group</b>	Management - PoE/PoE+ - Power over Ethernet

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



<b>Issue</b>	FI-190909
<b>Symptom</b>	In ICX7150 10G data port logged Micro flap detected but there is a no Physical link down
<b>Condition</b>	Every one sec syslog generated for Micro flap detected on 10G data port
<b>Workaround</b>	None
<b>Recovery</b>	
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.70 FI 08.0.90
<b>Technology / Technology Group</b>	System - Optics

<b>Issue</b>	FI-189130
<b>Symptom</b>	Avaya phones are not getting IP address assigned from ICX DHCP Server.
<b>Condition</b>	When ICX DHCP Server is configured with IP Telephony Data/Voice Server, Avaya phones are not getting dynamic IP address.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70 FI 08.0.61 FI 08.0.80
<b>Technology / Technology Group</b>	Management - DHCP (IPv4)

<b>Issue</b>	FI-108381
<b>Symptom</b>	No output displayed from the "show cable-diagnostics tdr x/x/x" command when issued from any stack unit other than the master unit.
<b>Condition</b>	None
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	High
<b>Found In</b>	
<b>Technology / Technology Group</b>	Management - Configuration Fundamentals

<b>Issue</b>	FI-190071
<b>Symptom</b>	Link status shown as down for port connected through 10G-SFPP-LRM-2-ADP .
<b>Condition</b>	Issue is seen only on non-Active Units after power cycle of the respective unit.
<b>Workaround</b>	
<b>Recovery</b>	Plug out and plug in the Cable recovers the issue.
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	System - Optics

## Issues

Closed with Code Changes in Release 08.0.90

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

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

<b>Issue</b>	FI-181579
<b>Symptom</b>	RADIUS Accounting request for user login does not have user-name attribute.
<b>Condition</b>	Accounting feature with RADIUS method is enabled for user login.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Security - RADIUS

<b>Issue</b>	FI-188485
<b>Symptom</b>	Occasionally flash access gets locked even after previous flash operation completed.
<b>Condition</b>	This issue happens when flash is accessed.
<b>Workaround</b>	Wait for 20 min before accessing flash again.
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - Configuration Fundamentals

<b>Issue</b>	FI-190380
<b>Symptom</b>	Clock Time Zone configuration is missing from running-config. With this fix we have enhanced the debugs to print stack trace when there is a change in the time zone .
<b>Condition</b>	After several weeks, the configuration is missing.
<b>Workaround</b>	Re-configure the timezone configuration.
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - NTP - Network Time Protocol

<b>Issue</b>	FI-190634
<b>Symptom</b>	Discrepancy in the RX Power value.
<b>Condition</b>	1. SFP is inserted without cable. 2. show optic output shows incorrect power values.
<b>Workaround</b>	Insert with cable.
<b>Recovery</b>	Insert with Cable.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-190384
<b>Symptom</b>	The ICX7750 device in SPX setup reloads by itself when trying to change inline-power through Web-GUI.
<b>Condition</b>	The user tries to change inline power of SPX using Web-GUI.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Management - PoE/PoE+ - Power over Ethernet

<b>Issue</b>	FI-181850
<b>Symptom</b>	When there are multiple ip subnets configured on the interface, the DHCP Server might not offer the IP address from the subnet of the secondary ip addresses.
<b>Condition</b>	Configure a DHCP server with multi-subnet VE
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - DHCP (IPv4)

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-185430
<b>Symptom</b>	On an extremely rare occasion, Apple MAC Book PC would not netboot with its iOS operating system.
<b>Condition</b>	The netboot-ing of Apple MAC PC with its operating system would fail and would not complete.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-190220
<b>Symptom</b>	Mac address table will not get updated when ports move from one vlan to another on single span environment. This will result in stale mac entries.
<b>Condition</b>	Enable single span. Add ports under one Vlan. On receiving traffic in those ports, the mac entries will get added with corresponding Vlan id. Move the ports to another Vlan . Now the previous mac entries learned through the old Vlan should get deleted and new mac entries should get added with the current Vlan id . But in issue state,mac address learned through old Vlan will not be removed / updated and will get deleted only on time out.
<b>Workaround</b>	NA
<b>Recovery</b>	NA
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Layer 2 Switching - VLAN - Virtual LAN

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

<b>Issue</b>	FI-187778
<b>Symptom</b>	During plug-out/plug-in of 10G ER/SR/LR optics, the show media ethernet interface output shows the optics as EMPTY.
<b>Condition</b>	When the optics are plugged out and plugged in, sometimes the show media ethernet cli output shows the optics as EMPTY
<b>Workaround</b>	Reloading the device resolves the issue.
<b>Recovery</b>	NA
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	System - Optics

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

<b>Issue</b>	FI-189579
<b>Symptom</b>	Copying of MACsec License into the ICX7750 was allowed even though this device doesn't support SW License
<b>Condition</b>	Copying of MACsec License into the ICX7750 will not be allowed, with suitable error message. At the same time it can be copied to PEs via 7750 SWs
<b>Workaround</b>	NA
<b>Recovery</b>	NA
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Management - Licensing

<b>Issue</b>	FI-189574
<b>Symptom</b>	During ICX7150 stack formation stack port flap and the device does not participate in stack.
<b>Condition</b>	The device not joined in stack, during ICX7150 stack formation.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.70 FI 08.0.90
<b>Technology / Technology Group</b>	Stacking

<b>Issue</b>	FI-189419
<b>Symptom</b>	Repeated issuance of 'copy running-config scp' command might make SSH not work.
<b>Condition</b>	The issue is seen only when 'copy running-config scp' command is issued repeatedly.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Management - SSH2 and SCP - Secure Shell and Copy

## Issues

Closed with Code Changes in Release 08.0.90

Issue	FI-189285
<b>Symptom</b>	After a factory reset, the ICX switch unable join the SZ controller. Received HTTP Response Code 400 from SZ server
<b>Condition</b>	With SZ configured and connected , do factory reset.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

Issue	FI-189218
<b>Symptom</b>	SSH session is not established and is abruptly terminated when x11 forwarding is enabled on client
<b>Condition</b>	SSH session is abruptly terminated when x11 forwarding is enabled on client with any KEX method
<b>Workaround</b>	NA
<b>Recovery</b>	NA
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.70 FI 08.0.61
<b>Technology / Technology Group</b>	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-189401
<b>Symptom</b>	When Broadcast/Multicast/unknown-unicast logging/dampening feature is configured on most of the interfaces and the MAC-filter is applied, the MAC-filter fails to add even though there are enough hardware resource available.
<b>Condition</b>	Broadcast/Multicast/unknown-unicast logging/dampening feature is configured on many interfaces and the MAC filter is being applied on the interface.
<b>Workaround</b>	None
<b>Recovery</b>	
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70 FI 08.0.61 FI 08.0.80
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

Issue	FI-188016
<b>Symptom</b>	Phone may not function sometimes as voice session is not established
<b>Condition</b>	When the phone session is established and device is not detected as phone through LLDP, phone doesn't get voice VLAN info from switch, so the phone voice session doesn't come up.
<b>Workaround</b>	Clear the sessions on the port, as LLDP message from phone builds the LLDP database, so next time session is established, the device is detected as phone.
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - 802.1x Port-based Authentication

<b>Issue</b>	FI-187481
<b>Symptom</b>	Syslog is displayed as "Error: invalid vlan 0"
<b>Condition</b>	When non-existent vlan name string is passed from Radius as part of user profile during dot1x/ mac-authentication on a flexauth enabled port
<b>Workaround</b>	not applicable as there is no functional impact
<b>Recovery</b>	not applicable as there is no functional impact
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - RADIUS

<b>Issue</b>	FI-187507
<b>Symptom</b>	Phone's voice vlan session is not created on a flexauth enabled port
<b>Condition</b>	On a flexauth enabled port, the issue is seen under following conditions 1. LLDP is enabled but CDP disabled 2. Server is down 3. Timeout-action is critical
<b>Workaround</b>	Configure both LLDP and CDP
<b>Recovery</b>	Enable both LLDP and CDP and clear the session to recover
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - MAC Port-based Authentication

<b>Issue</b>	FI-186567
<b>Symptom</b>	CDP phone is not automatically detected leading to manual configuration of phone from RADIUS server during authentication. Detection of CDP phones makes phones plug and play.
<b>Condition</b>	When device is not detected as phone and without RADIUS profile indicating the device as phone, treatment of phone when authentication fails or times-out, becomes inaccurate and phone may not function.
<b>Workaround</b>	Configure the RADIUS server for the device profiles with Phone using Ruckus VSA as phone, so the device is treated as phone
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-186541
<b>Symptom</b>	When invalid VLAN id or name is sent in attribute from RADIUS server, syslog message displays the message with VLAN id as 0, as such VLAN doesn't exist on the stack/switch
<b>Condition</b>	Sending invalid or not configured VLAN name or ID from RADIUS server during authentication triggers the syslog message displaying the name or ID as 0
<b>Workaround</b>	Send valid or configured VLAN name or ID in the RADIUS attributes during authentication
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-186125
<b>Symptom</b>	PC/Webauth Client does not get the DHCP IP address
<b>Condition</b>	When the uplink port is in standby/member unit of an ICX stack and it is member of a Vlan. And Admin has configured Webauth on the same vlan but has not enabled Webauth
<b>Workaround</b>	Enable Webauth and configure the uplink port as trust port
<b>Recovery</b>	Enable Webauth and configure the uplink port as trust port
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70 FI 08.0.61 FI 08.0.80
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-186854
<b>Symptom</b>	Client gets authenticated when invalid IPv6 ACLs are returned from RADIUS server
<b>Condition</b>	Client gets authenticated, though IPv6 ACL validation failed, as the validation failures are not checked in the right way, so the authentication succeeds
<b>Workaround</b>	Send only valid and/or configured IPv6 ACLs from RADIUS server during authentication
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - MAC Port-based Authentication

<b>Issue</b>	FI-189189
<b>Symptom</b>	SNMP-server configuration is lost after ICX device is rebooted.
<b>Condition</b>	SNMP-server command is configured with encrypted string length greater than 32 bytes.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.70 FI 08.0.61 FI 08.0.80
<b>Technology / Technology Group</b>	Management - SNMP - Simple Network Management Protocol

<b>Issue</b>	FI-189206
<b>Symptom</b>	Unexpected recurring reset of the switch when FIPS mode is enabled.
<b>Condition</b>	The reset occurs only when FIPS mode is enabled.
<b>Workaround</b>	Run the switch in non-FIPS or normal mode.
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Security - FIPS - Federal Information Processing Standards



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

<b>Issue</b>	FI-188498
<b>Symptom</b>	ICX device's own MAC-Address is shown in MAC-authentication table.
<b>Condition</b>	MAC-Authentication is enabled on the interface.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Security - MAC Port-based Authentication

<b>Issue</b>	FI-188544
<b>Symptom</b>	When BUM rate limits are configured on all the ports, stack loops might be observed.
<b>Condition</b>	BUM rate limiting is configured on all ports of a switch.
<b>Workaround</b>	None
<b>Recovery</b>	
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

<b>Issue</b>	FI-188212
<b>Symptom</b>	IGMP packets are dropped when IPSG is enabled.
<b>Condition</b>	IGMP packets are dropped when IPSG is enabled.
<b>Workaround</b>	None.
<b>Recovery</b>	
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	IP Multicast - IGMP - Internet Group Management Protocol

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-188610
<b>Symptom</b>	Switch may reload if BUM rate limits are configured on all ports of the switch/stack.
<b>Condition</b>	BUM rate limiting is configured on all ports of the respective unit
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

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

<b>Issue</b>	FI-188410
<b>Symptom</b>	MAC-Address truncated in the Syslog messages.
<b>Condition</b>	Issue is seen only for MAC authentication reject messages .
<b>Workaround</b>	N/A
<b>Recovery</b>	N/A
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Layer 2

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

<b>Issue</b>	FI-188130
<b>Symptom</b>	On ICX, suddenly PC connected to phone loss its connectivity
<b>Condition</b>	Flexauth enabled on port where PC and phone connected on it. Both are authenticated and at some instant PC lost its connectivity and stuck in vlan 4092 due to cable issues between phone and PC.
<b>Workaround</b>	Customer has to disable authentication for the port and add it back to resolve the issue.
<b>Recovery</b>	None
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - 802.1x Port-based Authentication

<b>Issue</b>	FI-188132
<b>Symptom</b>	Flexauth enabled port appears in auth-default-vlan as tagged port if the following sequence of events occur on these ports from a stack which has minimum of two units. 1. A vlan without any ports is configured as auth-default-vlan and few ports are configured for Flexauth. 2. Configuration is saved and reloaded. 3. After standby is elected, flexauth enabled ports are seen as tagged port in auth-default-vlan in standby unit
<b>Condition</b>	A Vlan without any port is configured as auth-default-vlan
<b>Workaround</b>	Auth-default-vlan needs to have at-least one static port
<b>Recovery</b>	Unconfigure and configure flexauth on the affected port again
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Security - MAC Port-based Authentication

<b>Issue</b>	FI-188364
<b>Symptom</b>	When RADIUS servers specified at port level, and any such RADIUS server is deleted from RADIUS configuration, authentication may not be attempted with other servers and timeout will take place
<b>Condition</b>	If any of the servers specified at the port level are deleted from configuration, the subsequent servers at the port level are attempted for authentication
<b>Workaround</b>	When RADIUS server is deleted from configuration, remove that server from all the ports where such server is specified for use
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

## Issues

Closed with Code Changes in Release 08.0.90

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

<b>Issue</b>	FI-188315
<b>Symptom</b>	When supportsave is issued more than once and if the first supportsave fails core file will get deleted.
<b>Condition</b>	1. Issue supportsave command to collect the core file. 2. GZIP fails to compress the file. 3. Core file is removed even when the supportsave fails. 4. Core file cannot be recovered by subsequent supportsave command.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.30
<b>Technology / Technology Group</b>	Management - Configuration Fundamentals

<b>Issue</b>	FI-188195
<b>Symptom</b>	Port Link doesn't come up when connected to multi gig ports of 7150-48ZP.
<b>Condition</b>	Devices connected On Multi-gig ports of 7150-48ZP doesn't come up due to auto negotiation failure .
<b>Workaround</b>	Configure 1000-full-slave on the ICX as a workaround
<b>Recovery</b>	N/A
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Management - PoE/PoE+ - Power over Ethernet

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

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

<b>Issue</b>	FI-187552
<b>Symptom</b>	A rare and unexpected reload of a member of a stack..
<b>Condition</b>	A race condition when message queues are accessed.
<b>Workaround</b>	None
<b>Recovery</b>	
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	System - System

<b>Issue</b>	FI-188186
<b>Symptom</b>	MAC-Auth keeps re-authenticating every 5 minutes even though 802.1X authentication is successful for the user with MAC-Auth followed by 802.1X authentication order configuration for PC users.
<b>Condition</b>	Though 802.1X authentication succeeds for user, the MAC-Auth session keeps re-authenticating every 5 minutes, as the default reauth-timeout for failed sessions is 5 minutes to avoid blocking users indefinitely when invalid profile is configured or some other issues.
<b>Workaround</b>	Increase reauth-timeout under authentication configuration to high value to reduce the frequent re-authentication of MAC-Auth session.
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

## Issues

Closed with Code Changes in Release 08.0.90

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

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

Issue	FI-187911
<b>Symptom</b>	In an SPX environment with a single CB, the power is not supplied to the end devices if they are connected to PE units.
<b>Condition</b>	This happens only to the devices connected to the PE ports and only if the SPX topology has single CB.
<b>Workaround</b>	No workaround available
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-187175
<b>Symptom</b>	TFTP access will not be allowed in the active
<b>Condition</b>	Issue will be simulated with the below steps. 1. Perform stack switch over when a TFTP running configuration download is in progress (via DHCP auto provision or CLI TFTP operations). 2. Perform second stack switch over which will not allow subsequent TFTP operations on the active device
<b>Workaround</b>	1. Other download mechanism like SCP, HTTPS can be used. 2. The switch over can be performed when TFTP operations have completed or DHCP auto provision is complete for running configuration download.
<b>Recovery</b>	Reload the device or perform the third switch over operation.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-186785
<b>Symptom</b>	Customer may experience high CPU processing in the network under certain rare conditions.
<b>Condition</b>	Under stress and scale conditions in the network, nexthop-movements may increase. These movements are processed in CPU causing high CPU.
<b>Workaround</b>	N/A
<b>Recovery</b>	N/A
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol

<b>Issue</b>	FI-186638
<b>Symptom</b>	When SNMP walk is done for IldpRemPortId in the Extreme switch, the output is HEX string for the interface name instead of text string.
<b>Condition</b>	When IldpRemPortId sub-type is configured as the value 5 (interfaceName) in ICX device and connected to the Extreme switch, the SNMP walk run in the Extreme side gives HEX string value for the interface.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	Management - SNMP - Simple Network Management Protocol

<b>Issue</b>	FI-186891
<b>Symptom</b>	Telnet from ICX7150 to Cisco ASA devices fail.
<b>Condition</b>	Cisco ASA negotiates to use terminal type for telnet access. Terminal-type command is not supported by ICX.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	Other - Other

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-187565
<b>Symptom</b>	When all the ports in lag is removed, the ICX device reloads spontaneously.
<b>Condition</b>	LAG is configured on an ICX device and all the ports in lag are removed.
<b>Workaround</b>	None
<b>Recovery</b>	
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	Layer 2 Switching - LAG - Link Aggregation Group

<b>Issue</b>	FI-186770
<b>Symptom</b>	1. When ICX is configured with a flow that should send PacketIn messages to the controller only when "no flow entries are matched", the ICX is instead sending PacketIn messages with the "reason" field set to "0" (NO_MATCH) when there is actually match with the flow entries 2. When ICX is configured with a flow that should send PacketIn messages to the controller only for packets that have matched flow entries, the ICX is sending PacketIn messages as expected but the reason code is set to "0" (NO_MATCH)
<b>Condition</b>	ICX is configured with a flow that should send PacketIn messages to the controller only when "no flow entries are matched" OR ICX is configured with a flow that should send PacketIn messages to the controller only for packets that have matched flow entries
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	SDN - OpenFlow

<b>Issue</b>	FI-187631
<b>Symptom</b>	The ACL show commands (e.g. show ip access-lists) display duplicate entries or missing entries when the show commands are issued from multiple sessions simultaneously.
<b>Condition</b>	The show commands are issued from multiple sessions simultaneously.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-187642
<b>Symptom</b>	OSPF neighborship stuck in EXSTART/EXCHG state.
<b>Condition</b>	When the interface is disabled and enabled and if opaque LSA is received, the OSPF neighborship stuck in EXSTART/EXCHG state.
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.70 FI 08.0.61 FI 08.0.30
<b>Technology / Technology Group</b>	Layer 3 Routing/Network Layer - OSPF - IPv4 Open Shortest Path First



<b>Issue</b>	FI-187838
<b>Symptom</b>	show version CLI doesn't work. Displays an information message and returns to the prompt.
<b>Condition</b>	Doesn't happen easily. Happened just once in a stacking setup after 3 days of longevity, which is basically just traffic forwarding w/o any triggers or configuration changes.
<b>Workaround</b>	None
<b>Recovery</b>	None identified so far.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Management - CLI - Command Line Interface

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

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

## Issues

Closed with Code Changes in Release 08.0.90

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

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

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

<b>Issue</b>	FI-187052
<b>Symptom</b>	An ACL is getting incorrectly configured on ports of standby unit, when user tries to remove/unbind an ACL that is not bound to those standby ports.
<b>Condition</b>	The issue happens on stacking setup only when 1. User tries to un-configure an ACL when there is no ACL bound to that port 2. If an ACL 'X' is configured on ports of standby unit and user incorrectly tries to remove ACL 'Y' on these ports then ACL 'Y' will replace ACL 'X' on these ports.
<b>Workaround</b>	None
<b>Recovery</b>	Apply some ACL on the impacted standby ports and then remove/unbind the ACL.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	

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

<b>Issue</b>	FI-183094
<b>Symptom</b>	On ICX7150-48 3 unit stack with Broadcast and multicast configuration of all 3 Units the ACL configurations not taking effected after reloaded the device
<b>Condition</b>	ACL configuration not taking effect once device reloaded
<b>Workaround</b>	Need to reapply the ACL configuration after reload
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

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

<b>Issue</b>	FI-186518
<b>Symptom</b>	Console connection to CB unresponsive for 25 seconds.
<b>Condition</b>	End SPX PE units in a ring become unreachable causing intermediate PEs in a ring to become unreachable as well, in a scaled up SPX deployment with large number of VLANs, MACs and STP instances.
<b>Workaround</b>	None.
<b>Recovery</b>	Console becomes responsive after 25 seconds.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Layer 2 Switching - xSTP - Spanning Tree Protocols

## Issues

Closed with Code Changes in Release 08.0.90

Issue	FI-186616
<b>Symptom</b>	Under rare circumstances, non active member of ICX7650 stack can stop showing the increments in port statistics.
<b>Condition</b>	Display of port statistics can stop incrementing in rare circumstances. This does not have any functional impact to the switching/routing capability.
<b>Workaround</b>	No workaround available.
<b>Recovery</b>	When ICX7650 gets into the above mentioned scenario, use "dm restart-bcm-counter" in the corresponding unit to recover from this state.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	

Issue	FI-186386
<b>Symptom</b>	Crash due to command "dm cpu filock clear"
<b>Condition</b>	command "'d cpu filock clear" when executed is crashing the device.
<b>Workaround</b>	N/A
<b>Recovery</b>	N/A
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	System - System

Issue	FI-185955
<b>Symptom</b>	If PD is not following standard and its getting detected as class 3 PD instead of class 4 during scanning mode. PD will get overloaded and will not get detected.
<b>Condition</b>	1. "inline power power-limit 30000" configured on interface connected to PD. 2. Class 4 PD does not follow standard and is set as class 3 PD during scanning mode.
<b>Workaround</b>	PoE controller decides that it should set port mode based on detection or based on configuration tho' the individual mask 0x39. "dm poe 1 set-mask 39 0" will set the individual mask 0x39 to 0. This enables PoE controller to use the configured class and PD will get detected.
<b>Recovery</b>	NA
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	Management - PoE/PoE+ - Power over Ethernet

Issue	FI-186693
<b>Symptom</b>	Ping from one device to another device present in same vlan is not successful.
<b>Condition</b>	1. Perform stack switch-over followed by write memory and Reload. 2. Ping from one device to the other device.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-186742
<b>Symptom</b>	Egress ACL applied on the Virtual Router Interface (VE), does not filter the traffic as per ACL rules on the PE ports of the vlan.
<b>Condition</b>	1. A PE port is part of more than 1 vlan 2. More than one vlan the PE port belongs have egress ACL applied on the Virtual router interface.
<b>Workaround</b>	If an egress ACL is to be applied on a virtual interface of a vlan with PE ports, then have the PE ports only in that single vlan. OR Apply Egress ACL on only one of the VEs the part is a member of
<b>Recovery</b>	1. Remove the given PE port from all the Vlans it is part of. 2. Add the PE port back to all the required vlans 3. Apply egress ACL only on one of the VEs
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-186782
<b>Symptom</b>	it observes a crash in the active unit.
<b>Condition</b>	User enters erase start and reload, it observed a crash.
<b>Workaround</b>	none.
<b>Recovery</b>	after the crash, it may recover.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Stacking - Mixed Stacking

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

<b>Issue</b>	FI-185942
<b>Symptom</b>	If SPX setup receives LLC packet with DSAP and SSAP values 0x8940 or 0x89CB, the packet is looped in the network.
<b>Condition</b>	SPX setup receives LLC packet with DSAP and SSAP values as 0x8940 or 0x89CB
<b>Workaround</b>	None
<b>Recovery</b>	
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.60
<b>Technology / Technology Group</b>	Security - Stack Management

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-186969
<b>Symptom</b>	ICX goes on reload , When "reload" button is submitted from web GUI while HTTPS download is in progress from CLI.
<b>Condition</b>	This issue occurs only with in below steps 1. Initiate a HTTPS download using the CLI command. For example: "copy https flash 10.10.10.10 icx.bin primary" 2. Open a web GUI interface for the device. 3. When HTTPS download in progress through CLI, clicks the reload button through web GUI interface
<b>Workaround</b>	Perform reload operation from other user interfaces or wait for download operation to complete before triggering the reload.
<b>Recovery</b>	NA
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-186983
<b>Symptom</b>	show interface brief " displays "state" as BLOCKING for linked-up interfaces on which spanning-tree is disabled and the interface's untagged VLAN is participating in xSTP.
<b>Condition</b>	Happens when spanning-tree is disabled on an interface first and then the interface's untagged VLAN starts participating in xSTP
<b>Workaround</b>	Disable spanning-tree on the interface only after enabling spanning-tree in the interface's untagged VLAN.
<b>Recovery</b>	Enable and disable spanning-tree on the interface after every time spanning tree is enabled on the interface's untagged VLAN.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	

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

<b>Issue</b>	FI-186492
<b>Symptom</b>	Control packet is not forwarded from a 7450-48F (active unit). When the input is received from a member or standby unit and it RCPUs the packet to a 7450-48F active.
<b>Condition</b>	Interpp filter outs the packet. 7450-48F have two packet processor, if the standby and member unit tries to RCPUs to the active unit, the control packet comes in one packet processor and tries to forward to another port on the 2nd processor. If the output port matches the interpp filter, it will get filter out.
<b>Workaround</b>	This issue has to match the configuration in the topology, in this case, tries to avoid using */3/4 port because it matches the port ID of the interpp link.
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-186565
<b>Symptom</b>	if an abrupt switch over or failure open, ACL rules might not be complete if hot swap was in progress.
<b>Condition</b>	switch over or fail over while ACL hot swap is in progress.
<b>Workaround</b>	reload the units to make sure hot swap is complete.
<b>Recovery</b>	reload the units to make sure hot swap is complete.
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

<b>Issue</b>	FI-186565
<b>Symptom</b>	if an abrupt switch over or failure open, ACL rules might not be complete if hot swap was in progress.
<b>Condition</b>	switch over or fail over while ACL hot swap is in progress.
<b>Workaround</b>	reload the units to make sure hot swap is complete.
<b>Recovery</b>	reload the units to make sure hot swap is complete.
<b>Probability</b>	Low
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

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

## Issues

Closed with Code Changes in Release 08.0.90

<b>Issue</b>	FI-185957
<b>Symptom</b>	The message "INFO: all 2 display buffers are busy, please try later." will be displayed in the show command output, instead of expected functionality output. (Example show commands: "show stack", "show version")
<b>Condition</b>	Seen when all below conditions are met 1. The DUT is a scaled setup with huge data to display in show command 2. Two or more telnet/ssh sessions are connected. 3. The show command is performed in two sessions and output is pending for user input in the page mode in both the sessions. 4. The show command performed in the new session will show the error message "INFO: all 2 display buffers are busy, please try later."
<b>Workaround</b>	Abort the pending show command by pressing "Ctrl + c" in one of the two sessions or by completing the output display before performing the show command in new session. If the sessions are abruptly closed without completing the pending output, reload of the device is required
<b>Recovery</b>	NA
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	Cloud Management - Cloud Agent

<b>Issue</b>	FI-185696
<b>Symptom</b>	In untagged VLAN open flow hybrid port for unprotected VLAN, a flow with out VLAN id gets added though its not supported.
<b>Condition</b>	When VLAN is configured as protected , the flow without VLAN id is accepted and installed . When the port is turned to unprotected, previously installed flow still persists.
<b>Workaround</b>	VLAN should not be changed from protected to unprotected mode when flow without VLAN id is configured .
<b>Recovery</b>	NA
<b>Probability</b>	
<b>Found In</b>	FI 08.0.61
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-185853
<b>Symptom</b>	Port Link shown as down when connected to multi gig port of 7150ZP
<b>Condition</b>	Devices connected on multi gig ports of 7150ZP doesn't come up due to auto negotiation failure .
<b>Workaround</b>	configure the multi-gig port as 1000-full-slave as a workaround.
<b>Recovery</b>	None
<b>Probability</b>	High
<b>Found In</b>	
<b>Technology / Technology Group</b>	



<b>Issue</b>	FI-181567
<b>Symptom</b>	On very rare occasions, during ICX7650 reload, system can encounter an unexpected kernel exception error with following message in console and not able to proceed further in the boot sequence. Sample error message: [ 51.081969] iproc-idm idm: idm_aci_pcie_s1 ( 1 21005900 358) fault
<b>Condition</b>	This condition was observed only when ICX7650 was reloaded back to back in a tight loop for several hours. Not seen with the normal scenarios when system is in steady state.
<b>Workaround</b>	None
<b>Recovery</b>	Reset the power for the failed unit if it is stuck in the same state.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-185913
<b>Symptom</b>	Under rare circumstances, when a stack switch-over is performed, the unit transitioning from active role to standby role crashes and boots back up.
<b>Condition</b>	FlexAuth is enabled and active on the system, and FlexAuth sessions are learned on ports across many Stacking and SPX units.
<b>Workaround</b>	None
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.70 FI 08.0.80
<b>Technology / Technology Group</b>	

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

<b>Issue</b>	FI-185648
<b>Symptom</b>	When authenticated clients already exist on port in a VLAN, subsequent failed clients can't be moved to Restricted VLAN, so the syslog message prints the existing session count, which is confusing
<b>Condition</b>	When an authenticated client exists and another clients fails, the syslog message is displayed
<b>Workaround</b>	None
<b>Recovery</b>	None
<b>Probability</b>	
<b>Found In</b>	
<b>Technology / Technology Group</b>	

## Issues

### Known Issues in Release 08.0.90a

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

<b>Issue</b>	FI-184049
<b>Symptom</b>	High CPU resulting in ssh/telnet session or ping becoming unresponsive.
<b>Condition</b>	Continuous high number of Non-IP-multicast packets or un-known multicast packets ingressing on ICX 7xxx switches with default or any configuration. These packets are punted to CPU on lookup failure in the L2 table and classified as un-known multicast packets.
<b>Workaround</b>	
<b>Recovery</b>	
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	Traffic Management - Rate Limiting and Shaping

## Known Issues in Release 08.0.90a

This section lists open software issues with Critical, High, and Medium Technical Severity in FastIron 08.0.90a.

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

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

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

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

## Known Issues in Release 08.0.90

This section lists open software issues with Critical, High, and Medium Technical Severity in FastIron release 08.0.90.

Issue	FI-195702
<b>Symptom</b>	"show ipv6 dhcp6-server lease" command does not reflect all the leases that have been issued by the DHCPv6 server running on ICX. Only some or none of the leases may be shows. Also, when an existing lease information expires for a device, it might be assigned a different IP (as opposed to the IP it is trying to renew)
<b>Condition</b>	This issue will be seen in ICX 7K devices running FI 08.0.90 after the device reloads (in stand-alone devices) or after switchover/failover (in stacking topologies)
<b>Workaround</b>	None
<b>Recovery</b>	No manual recovery is operationally necessary. Even though the lease information stored by the DHCPv6 server is not complete, it will not assign the same IP to multiple devices. During address assignment, before assigning an IP, the server will ensure that no other device it has serviced is using the IP it is going to assign to a new device.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

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

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

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

<b>Issue</b>	FI-194591
<b>Symptom</b>	When SmartZone is reachable through a management-vrf, ICX is not able to establish a session with SmartZone. SmartZone will be unable to monitor the ICX device. The following Syslog will be seen on the ICX when trying to connect to SmartZone - Feb 12 10:55:46:!:SZAgent: SZ Query to SZ-IP Failed. Reason: HTTPS Connection Error
<b>Condition</b>	Seen in images FI 08.0.80 and above, when SmartZone is reachable through the management-vrf and management-vrf is configured similar to the example below -  interface management 1  vrf forwarding test  no ip dhcp-client enable  ip address <IP> <SubnetMask> !
<b>Workaround</b>	NA
<b>Recovery</b>	NA
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80 FI 08.0.90
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-193944
<b>Symptom</b>	A series of IDM error may be seen with the message "iprocs-idm idm: idm_hs_apbs (41 67019900 414) fault"
<b>Condition</b>	On rare occasions, when USB mass storage device is plugged out, a series of IDM error may be seen.
<b>Workaround</b>	No workaround available.
<b>Recovery</b>	System recovers itself with an automatic reboot.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

## Issues

### Known Issues in Release 08.0.90

<b>Issue</b>	FI-192861
<b>Symptom</b>	ICX7850-48FS may show a series of IDM fault message like "[ 8983.951661] iproc-idm idm: idm_pcie_0_ds11 ( 5 21009900 367) fault" and LED behavior may be affected. On rare conditions system might reload to recover.
<b>Condition</b>	When used with macsec traffic in ICX7850-48FS, system may show a series of IDM fault message like "[ 8983.951661] iproc-idm idm: idm_pcie_0_ds11 ( 5 21009900 367) fault" and LED behavior may be affected. On rare conditions system might reload to recover.
<b>Workaround</b>	Not configuring MACSEC in ICX7850-48FS can prevent this issue.
<b>Recovery</b>	system might automatically reload to recover.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

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

<b>Issue</b>	FI-192622
<b>Symptom</b>	in a scale setup with 12 unit stack, if user tries to unconfigure all, telnet session can be timeout.
<b>Condition</b>	unconfigure the stack in a scale setup
<b>Workaround</b>	reconnect to the telnet session when the timeout happen.
<b>Recovery</b>	reconnect to the telnet session when the timeout happen.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	

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

<b>Issue</b>	FI-187670
<b>Symptom</b>	In multiple-untagged mode and with multiple Mac-Auth/802.1X sessions having dynamic ACLs and using the same User ACL for all sessions, any change of User ACL definitions (addition/deletion of filters in ACL) may cause high CPU usage.
<b>Condition</b>	With multiple sessions using the same User ACL, any filter change triggers unbinding of old filters and binding of new filters for all the sessions on that port. Depending on the number of sessions and number of filters in the User ACL, the time consumed to program ACL filters in TCAM may take significant time causing the console/telnet/ssh access to hang until the operation is complete.
<b>Workaround</b>	There is no workaround and the only way to prevent is not changing the User ACLs or having less number of MAC-Auth/802.1X sessions on a port and/or less number of filters in the User ACL
<b>Recovery</b>	There is no recovery for this symptom
<b>Probability</b>	
<b>Found In</b>	FI 08.0.80
<b>Technology / Technology Group</b>	

<b>Issue</b>	FI-123259
<b>Symptom</b>	If ACL configurations such as adding/deleting ACL, adding/deleting filters and bind/unbind of ACLs to PE ports are done while the PE Hot-Swap is in progress, it can result in unpredictable behavior for that PE such as filter IDs to be out-of-sync with active, ACL not getting bound to ports... etc.
<b>Condition</b>	ACL configuration changes on the active when PE hot-swap is in progress.
<b>Workaround</b>	
<b>Recovery</b>	Reload of the PE.
<b>Probability</b>	Medium
<b>Found In</b>	FI 08.0.95
<b>Technology / Technology Group</b>	Security - ACLs - Access Control Lists

<b>Issue</b>	FI-177848
<b>Symptom</b>	This problem happens in a scaled scenario where we have either exhausted the TCAM or adding a new filter to an ACL used for a PBR route-map will result in exhausting the TCAM resource. In this scenario, user does not get an error when adding a filter to the ACL which is used in PBR route-map. But the new filter does not get reflected in the TCAM as TCAM resource is exhausted. This applies to ACLs that are used in PBRv4 as well as PBRv6 route-maps.
<b>Condition</b>	Adding a filter in ACL which is used by PBR/PBRv6, when TCAM resource are exhausted or in the verge of getting exhausted.
<b>Workaround</b>	No workaround.
<b>Recovery</b>	User can add new filter after freeing up some TCAM space by deleting some existing ACL rules. The ACL rules that need to be freed up can be across any ACLs in the system and not just the ones used for PBR route-maps.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.95
<b>Technology / Technology Group</b>	

## Issues

### Known Issues in Release 08.0.90

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

<b>Issue</b>	FI-181286
<b>Symptom</b>	User might see i2c error messages displayed in console when plugging in or when accessing an unsupported SFPP. Sample error message: I2C_CORE: B80:D51 Read Failed.Bytes read=0 Bytes to read=1.
<b>Condition</b>	User might see i2c related error messages, when plugging in an unsupported SFPP. This was observed on SFPP with part name: AFBR-707ASDZ-BR2
<b>Workaround</b>	Please use only supported SFPP.
<b>Recovery</b>	Replace any unsupported SFPP in the unit with a supported one.
<b>Probability</b>	
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Other - Other

<b>Issue</b>	FI-201087
<b>Symptom</b>	PE candidates are not discovered.
<b>Condition</b>	CB is running an 08.0.90 image or later. PE candidates are running a pre-08.0.90 image.
<b>Workaround</b>	
<b>Recovery</b>	Upgrade all PE candidates to an 08.0.90 image or later to match the image used by the CB before entering the <b>spx interactive-setup</b> command or before configuring zero-touch-enable in spx cb-configure mode.
<b>Probability</b>	100%
<b>Found In</b>	FI 08.0.90
<b>Technology / Technology Group</b>	Layer 2 - Switch Port Extender





© 2020 CommScope, Inc. All rights reserved.  
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
[www.ruckuswireless.com](http://www.ruckuswireless.com)