RELEASE NOTES

FastIron 08.0.90 for Ruckus ICX Switches Release Notes Version 1

Supporting FastIron 08.0.90

Part Number: 53-1005579-01
Publication Date: 20 February 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Document History

Version	Summary of changes	Publication date
FastIron 08.0.90 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

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. This release enhances Ruckus SmartZone management of ICX switches, enabling the configuration of ICX switches from SmartZone (requires SmartZone release 5.1.1). A number of 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@arris.com.

When contacting us, include the following information:

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

For example:

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

Ruckus Product Documentation Resources

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

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

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

Online Training Resources

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

Contacting Ruckus Customer Services and Support

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

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

What Support Do I Need?

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

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

Open a Case

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

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.

- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

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

Self-Service Resources

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

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

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

New in This Release

Hardware

The following section lists new hardware introduced with this release 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-admin

  The default username and password apply to all forms of access including Console, SSH and WEB2. The administrator will be prompted to create a new password after logging in. ICX devices that are already deployed with a previous release and upgraded to 08.0.90 will not be affected by this change.
- **SSH enabled out of the box**: SSH is now enabled and Telnet is disabled by default on switches that do not have a statrtup-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, 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 08.0.90

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, 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.

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.

Feature	Descriptions
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.
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.
SmartZone-based ICX configuration management	FastIron 08.0.90, used in conjunction with SmartZone 5.1.1, provides the capability to view and change ICX switch settings from SmartZone.

CLI Commands

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

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**
- **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**
- **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

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)

Supported Power Supplies

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

Supported Optics

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

Software Upgrade and Downgrade

Image File Names

Download the following images from www.ruckuswireless.com.

Device	Boot image file name	Flash image file name	UFI file name (boot, image)
ICX 7150	mnz10115.bin	SPR08090.bin/SPS08090.bin	SPR08090ufi.bin/SPS08090ufi.bin
ICX 7250	spz101115.bin	SPR08090.bin/SPS08090.bin	SPR08090ufi.bin/SPS08090ufi.bin
ICX 7450	spz10115.bin	SPR08090.bin/SPS08090.bin	SPR08090ufi.bin/SPS08090ufi.bin
ICX 7650	tnu10115.bin	TNR08090.bin/ TNS08090.bin	TNR08090ufi.bin/TNS08090ufi.bin
ICX 7750	swz10115.bin	SWR08090.bin/ SWS08090.bin	SWR08090ufi.bin/SWS08090ufi.bin
ICX 7850	n/a	n/a	TNR08090ufi.bin

PoE Firmware Files

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

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

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

NOTE

Please note the following recommendations and notices:

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

Open Source and Third Party Code

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

Manufacturer	Third Party Software
InMon	Sflow
Broadcom Inc	SDK 6.5.6
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: • ICX7150, ICX7250, ICX7450: Linux 4.4 • ICX7650, ICX7850: Linux 3.14.65 • ICX7750: Linux 2.6.34.6
Aquantia Inc	Aquantia phy driver AQR API 2.1.0
Aquantia	Aquantia phy drivers: • ICX7150: AQR 3.5.E • ICX7450: AQR 2.C.5 • ICX7650: AQR 3.5.E • ICX7750: AQR 1.38.11

Manufacturer	Third Party Software
open source S/W	Parted utility
Broadcom Inc	Miura Phy driver 1.5
Broadcom Inc	EPDM driver 1.5.1
Spansion	Flash driver
http://www.bzip.org/	Bzip
http://www.hackersdelight.org/	Integer square root computation
GNU (http://www.gnu.org/)	LZMA SDK (compression method)
Freescale (NXP)	Software for PowerPC chip
Open Source SW	openssl_tpm_engine-0.4.2
Open Source SW	tpm-tools-1.3.8
Open Source SW	trousers-0.3.11.2
Infineon Technologies AG	ELTT_v1.3
Allegro Software	HTTP/HTTP-S, SSHv2
WindRiver	SNMPv1,v2c,v3; IPSecure
Interlink	Radius
SafeNet Sentinel RMS	Software Licensing Code - SafeNet Sentinel RMS
open source S/W	NSS 3.12.4 with NSPR 4.8
open source S/W	OpenSSL FIPS Object Module v2.0.5
open source S/W	OpenSSL crypto Ver 1.0.1e
GubuSoft	Javascript based tree display
GubuSoft	Javascript based tree display
GNU (The Regents of the University of California)	Syslog
BSD(The Regents of the University of California)	DNS Query/Resolution
BSD(The Regents of the University of California)	TimeZone Code (SNTP)
BSD(The Regents of the University of California)	Router Renumbering
BSD(The Regents of the University of California)	IPv6 defines
RouterWare Inc	TCP/IP stack, IPX, OSPFv2, TELNET, STP, LSL, TFTP client, BOOTP client and relay
IP Infusion	RIPng, OSPFv3, BGP4
open source S/W	libunwind
Wind River Systems, Inc.	Wind River MIB Compiler, version 10.2

Issues

Closed with Code Changes in Release 08.0.90

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

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

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

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

Issue	FI-193003
Symptom	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] "
Condition	NA
Workaround	Reload of the switch resolved the error and cli worked fine after reload.
Recovery	NA
Probability	Low
Found In	FI 08.0.30
Technology / Technology Group	System - System

Issue	FI-193462
Symptom	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
Condition	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.
Workaround	No workaround available.
Recovery	No recovery needed. It automatically recovers
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Other - Other

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

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

Issue	FI-192861
Symptom	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.
Condition	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.
Workaround	Not configuring MACSEC in ICX7850-48FS can prevent this issue.
Recovery	system might automatically reload to recover.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Other - Other

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

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

Issue	FI-191512
Symptom	While running power line disturbance tests, the SSH host key stored on the flash is lost
Condition	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
Workaround	NA
Recovery	Re-generate SSH key files
Probability	Low
Found In	FI 08.0.61 FI 08.0.90
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-192003
Symptom	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.
Condition	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.
Workaround	When configuring the ports, using 'to' keyword would prevent the issue from happening.
Recovery	
Probability	High
Found In	FI 08.0.70
Technology / Technology Group	Layer 2 Switching - VLAN - Virtual LAN

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

Issue	FI-191216
Symptom	Traffic dropped by Default Null Route despite better eBGP Default Route
Condition	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.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.80
Technology / Technology Group	Layer 3 Routing/Network Layer - BGP4 - IPv4 Border Gateway Protocol

Issue	FI-190837
Symptom	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.
Condition	one or more PoE HWs are sensing voltage drift. This HW may or may not recover.
Workaround	move to 8070d
Recovery	move to 8070d
Probability	Low
Found In	FI 08.0.70 FI 08.0.90
Technology / Technology Group	Management - PoE/PoE+ - Power over Ethernet

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

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

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

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

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

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

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

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

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

Issue	FI-190380
Symptom	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 .
Condition	After several weeks, the configuration is missing.
Workaround	Re-configure the timezone configuration.
Recovery	None
Probability	Low
Found In	FI 08.0.90
Technology / Technology Group	Management - NTP - Network Time Protocol

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

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

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

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

Issue	FI-190220
Symptom	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.
Condition	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.
Workaround	NA
Recovery	NA
Probability	Low
Found In	FI 08.0.30
Technology / Technology Group	Layer 2 Switching - VLAN - Virtual LAN

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

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

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

Issue	FI-189579
Symptom	Copying of MACsec License into the ICX7750 was allowed even though this device doesn't support SW License
Condition	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
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.70
Technology / Technology Group	Management - Licensing

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

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

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

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

Issue	FI-189401
Symptom	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.
Condition	Broadcast/Multicast/unknown-unicast logging/dampening feature is configured on many interfaces and the MAC filter is being applied on the interface.
Workaround	None
Recovery	
Probability	High
Found In	FI 08.0.70 FI 08.0.61 FI 08.0.80
Technology / Technology Group	Security - ACLs - Access Control Lists

Issue	FI-188016
Symptom	Phone may not function sometimes as voice session is not established
Condition	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.
Workaround	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.
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	Security - 802.1x Port-based Authentication

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

Issue	FI-187507
Symptom	Phone's voice vlan session is not created on a flexauth enabled port
Condition	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
Workaround	Configure both LLDP and CDP
Recovery	Enable both LLDP and CDP and clear the session to recover
Probability	High
Found In	FI 08.0.70
Technology / Technology Group	Security - MAC Port-based Authentication

Issue	FI-186567
Symptom	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.
Condition	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.
Workaround	Configure the RADIUS server for the device profiles with Phone using Ruckus VSA as phone, so the device is treated as phone
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

Issue	FI-186541
Symptom	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
Condition	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
Workaround	Send valid or configured VLAN name or ID in the RADIUS attributes during authentication
Recovery	
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

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

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

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

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

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

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

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

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

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

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

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

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

Issue	FI-188130
Symptom	On ICX, suddenly PC connected to phone loss its connectivity
Condition	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.
Workaround	Customer has to disable authentication for the port and add it back to resolve the issue.
Recovery	None
Probability	Low
Found In	FI 08.0.70
Technology / Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-188132
Symptom	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
Condition	A Vlan without any port is configured as auth-default-vlan
Workaround	Auth-default-vlan needs to have at-least one static port
Recovery	Unconfigure and configure flexauth on the affected port again
Probability	High
Found In	FI 08.0.70
Technology / Technology Group	Security - MAC Port-based Authentication

Issue	FI-188364
Symptom	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
Condition	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
Workaround	When RADIUS server is deleted from configuration, remove that server from all the ports where such server is specified for use
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

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

Issue	FI-188315
Symptom	When supportsave is issued more than once and if the first supportsave fails core file will get deleted.
Condition	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.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology / Technology Group	Management - Configuration Fundamentals

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

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

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

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

Issue	FI-188186
Symptom	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.
Condition	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.
Workaround	Increase reauth-timeout under authentication configuration to high value to reduce the frequent re-authentication of MAC-Auth session.
Recovery	None
Probability	
Found In	FI 08.0.70
Technology / Technology Group	

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Issue	FI-183094
Symptom	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
Condition	ACL configuration not taking effect once device reloaded
Workaround	Need to reapply the ACL configuration after reload
Recovery	None
Probability	High
Found In	FI 08.0.90
Technology / Technology Group	

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

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

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

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

Issue	FI-185955
Symptom	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.
Condition	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.
Workaround	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.
Recovery	NA
Probability	Medium
Found In	FI 08.0.61
Technology / Technology Group	Management - PoE/PoE+ - Power over Ethernet

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Issue	FI-185648
Symptom	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
Condition	When an authenticated client exists and another clients fails, the syslog message is displayed
Workaround	None
Recovery	None
Probability	
Found In	
Technology / Technology Group	

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

Issue	FI-184049
Symptom	High CPU resulting in ssh/telnet session or ping becoming unresponsive.
Condition	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.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.80 FI 08.0.90
Technology / Technology Group	Traffic Management - Rate Limiting and Shaping

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
Symptom	"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)
Condition	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)
Workaround	None
Recovery	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.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	

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

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

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

Issue	FI-194591
Symptom	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:I:SZAgent: SZ Query to SZ-IP Failed. Reason: HTTPS Connection Error
Condition	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> !
Workaround	NA
Recovery	NA
Probability	
Found In	FI 08.0.80 FI 08.0.90
Technology / Technology Group	

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

Issue	FI-192861
Symptom	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.
Condition	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.
Workaround	Not configuring MACSEC in ICX7850-48FS can prevent this issue.
Recovery	system might automatically reload to recover.
Probability	
Found In	FI 08.0.90
Technology / Technology Group	Other - Other

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

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

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

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

Issue	FI-123259
Symptom	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.
Condition	ACL configuration changes on the active when PE hot-swap is in progress.
Workaround	
Recovery	Reload of the PE.
Probability	Medium
Found In	FI 08.0.95
Technology / Technology Group	Security - ACLs - Access Control Lists

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

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

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

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