# FastIron 08.0.70c for Ruckus ICX Switches

## Release Notes Version 2

25 October 2018

# Contents

# Document history

| Version | Summary of changes | Publication date |
| --- | --- | --- |
| FastIron 08.0.70c for ICX Switches Version 2 | Section for important changes in 08.0.70c added. | 25 October 2018 |
| FastIron 08.0.70c for ICX Switches Version 1 | New feature and bug fixes. | 4 September 2018 |

# Preface

## 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 Networks products, and customers and partners with active support contracts.

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

## Ruckus 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 documentation by product or perform a text search. Access to Release Notes requires an active support contract and Ruckus Support Portal user account. Other technical documentation content is available without logging into the Ruckus Support Portal.

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

## Document feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at: docs@ruckuswireless.com.

When contacting us, please include the following information:

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

For example:

- Ruckus Small Cell Alarms Guide SC Release 1.3
- Part number: 800-71306-001
- Page 88

# Overview

Ruckus FastIron release 08.0.70 introduces the Ruckus ICX 7650, the first stackable switch to support 100-GbE uplinks. The Ruckus ICX 7650 is available with full Multigigabit Ethernet access ports, 10-GbE aggregation ports, and a choice of 10-GbE, 40-GbE, or 100-GbE uplinks, setting the bar higher for flexibility and scalability. The ICX 7650 Z-Series delivers class-leading Multigigabit port density capable of 1, 2.5, 5, or 10 GbE speeds. The ICX 7650 also offers 256-bit MACsec encryption.

Ruckus FastIron release 8.0.70 adds Campus Fabric capability to the ICX 7150 switch family, better enabling mobility, security, and application agility for campus networks. IPsec encryption on the ICX 7450 adds support for IPv6 and is CSFC certified. Ruckus FastIron release 08.0.70 also meets the criteria for federal deployments and will be officially released supporting the FIPS, CC, USGv6, and JITC certification standards for all ICX 7K platforms.

# 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.

### New switch

| | |
|---|---|
| Product name | Ruckus ICX 7650 Switch |
| Description | Ruckus ICX 7650 Switch is designed to meet the new challenges of the multigigabit wireless era. It delivers non-blocking performance, high availability, and scalability with Multigigabit Ethernet access, high PoE output as well as 10 Gigabit Ethernet Aggregation and 10G/40G/100G uplink options. |
| Product features | <ul><li>Up to 2x 40 GbE uplink or 4x 40GbE stacking ports</li><li>Up to 2x 100 GbE uplink or stacking ports</li><li>Up to 24x 1/2.5/5/10G Multigigabit Ethernet ports</li><li>Dual load sharing power supplies for system power redundancy</li><li>Redundant uplink/stacking ports</li><li>Instantaneous hitless failover to a standby controller</li><li>Stack level ISSU for continuous operations</li><li>Hot-insertion/removal of stack members to avoid service interruption</li><li>PoE+/802.3bt up to 90W per port (Up to 90W per port, IEEE 802.3bt standard pending ratification. Compatible with uPoE.)</li><li>Up to 1500W PoE budget with two power supplies</li><li>IPv4 and IPv6</li></ul> |

- BGP, OSPF, VRRP, PIM, PBR, VRF

## Software features

The following section lists new, modified, and deprecated software features for this release. For information about which platforms support these features, refer to the *FastIron Features and Standards Support Matrix*, available at www.ruckuswireless.com.

### New software features for 08.0.70c

The following enhancements are introduced in this release:

- **PoE Updates and Related Syslog Messages**—PoE functionality on some ports will not be available when device (PoE chip) fails during operation. These ports show up as internal hardware fault in the **show inline power** command output. In such scenarios, remove the PDs and configure the **no inline power** command on the affected ports. A syslog message is generated that shows the specific ports that are offline due to device fail.
- **Link Dampening and Alarms**—The **linkdampen** command is introduced on ICX 7150 devices to allow the user to define sampling periods for link dampening on a port. Microflaps detected on the interface and related changes in state are reported through system logs and in **show interfaces ethernet** command output so that the user can determine when a response is necessary. The **linkdampen** command can coexist on the same interface with the **link error disable** link dampening command.
- **Debug Data Collection**—Debug logs are automatically collected when a port goes down and are stored in the console log file. Supported on the ICX 7150 only.

### New software features for 08.0.70b

The following enhancements are introduced in this release:

- **Multiple S-VLAN Support**—A maximum of 50 SVLANs can be configured on an interface.
- **BPDU Scaling**—Scaling improvements for BPDU tunneling.
- **PoE Data Link Decoupling**—data link operation is decoupled from inline power by default. In the default state, the datalink operational behavior on a PoE port does not affect the power state of the powered device that is connecting to the port.

### New software features for 08.0.70a

FastIron release 08.0.70a contains defect fixes only. There are no features or enhancements in this release.

### New software features for 08.0.70

The following software features and enhancements are introduced in this release.

- **Terminal logging**—Console logging feature captures all the console prints generated on the system to a RAMFS file and upon certain triggers copies the RAMFS file to the flash memory.
- **Reset button to factory default settings**
- **Status button support**— To select the status mode to display the corresponding status on the individual port status LED, you can press the status mode selection button.

- **Auto PoE firmware upgrade**—PoE firmware is bundled with FastIron image and is automatically installed or upgraded as part of unit bootup. That is, manual intervention is not required to choose the corresponding firmware version for each FastIron image version.
- **PoE enabled by default**—PoE is enabled by default and power is automatically allocated to all PoE-capable ports on bootup. As the 'inline power' configuration is applied on all PoE-capable ports by default, PD is powered up as soon as it is connected to the port.
- **System backup to USB**— Allows to copy files from the system flash memory to the connected USB drive.
- **Boot from USB**—Software upgrade can be done through manifest file download using USB drive.
- **PKI authentication for Syslog and RADIUS**
- **Auto image upgrade for PE**—Standalone units with a different software image can be upgraded to the correct image before being converted to PEs.
- **Staggered upgrade for Campus Fabric**—An in-service software upgrade (ISSU) allows units in a Campus Fabric system to be upgraded with minimal interruptions to multi-unit topologies.
- **ICX 7150 as a PE in a Campus Fabric network**—All ICX 7150 models can be configured as PE units. SPX LAGs on ICX 7150 PEs are limited to eight ports.
- **DHCP generic options**—The list of supported DHCP server options has been extended significantly, providing more scope for DHCP client provisioning and configuration.
- **VRF over MCT**—VRF over MCT allows the peer cluster devices to maintain separate routing and forwarding tables for each VRF instance, thus allowing overlapping of IP addresses, route isolation, and so on.
- **Q-in-Q BPDU tunneling**—Protocol/BPDU tunneling over Q-in-Q enables the service provider to provide Layer 2 VPN connectivity between different customer sites. This facilitates the service provider to give the customers an infrastructure to run various Layer 2 protocols and connect to all geographically-separated sites.
- **Selective Q-in-Q**—Selective Q-in-Q is the way to achieve Q-in-Q per CVLAN basis, where you have the flexibility to selectively choose and add service a VLAN tag based on the customer VLAN.
- **VXLAN support**—ICX 7750 devices support Virtual Extensible Local Area Network (VXLAN) technology, which creates a logical Layer 2 network overlaying a Layer 3 IP network.
- **PVLAN with LAG**—Private VLAN support over LAG port enhances the bandwidth on promiscuous, ISL and host links and increases link reliability.
- **Wrapper for adding/removing selective VLANs**—The new wrapper enables the addition and deletion of tagged ports selectively to a VLAN at the interface level.
- **Keychain for OSPF**—Keychain provides a mechanism to ensure key rollover based on the lifetime or duration specified for each key used for authentication.
- **IPv6 support for IPsec**—IPv6 over IPsec tunnel feature support enables to get the IPsec Fed certification.
- **NAT transversal for IPsec**—Network Address Translation (NAT) is a method to remap a private IP address to public IP address by modifying the address information in the IP packet. The remapping is performed by the transit routers, when the traffic passes through them.
- **PKI Support for IKE**—Public Key Infrastructure (PKI) provides certificate management to support secured communication for security protocols such as IP security (IPsec), thus ensuring customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network.

- **IPv6 PBR support**— IPv6 Policy-Based Routing (PBR) allows you to manually configure how IPv6 packets that match certain criteria can be forwarded instead of following the IPv6 Routing Table Manager (RTM) routes.
- **SSH Rekey**—SSH rekeying is the process of exchanging the session keys at a configured interval, either in terms of time limit or data limit for a SSH session. SSH rekeying is triggered when the maximum minutes has reached or when the maximum number of packets transmitted has reached for a session.
- **Self-authenticated upgrade (SAU) licensing for the ICX 7650**—Self-Authenticated Upgrade (SAU) licensing allows you to upgrade or downgrade to a licensed feature set with a single command.
- **Zero-touch provisioning enhancements**—Both zero-touch provisioning and SPX interactive-setup can interoperate between major releases, and zero-touch provisioning can be triggered at any CPU rate.
- **Egress ACL accounting**—ACL accounting is now supported on inbound and outbound ACLs.
- **No port shutdown for "restrict" option of port mac security**
- **BGP over IPSec**

## CLI commands

### New commands in 08.0.70bc

The following commands are modified in this release:

- inline power
- linkdampen
- show inline power

### New commands in 08.0.70b

The following commands are new in this release:

- inline power couple-datalink

### New commands in 08.0.70a

There are no new, modified, or deprecated commands in FastIron release 08.0.70a.

### New commands

The following commands are new in this release:

- accept-lifetime
- area authentication (OSPFv3)
- area virtual-link authentication (OSPFv2)
- area virtual-link authentication (OSPFv3)
- authentication-algorithm
- clear l2protocol dot1q-tunnel counters
- default-acl

- ip arp port-move-syslog
- ip ospf authentication
- ip ospf authentication keychain
- ip ssh rekey
- ip ssh key-exchange-method dh-group1-sha1
- ipv6 ospf authentication
- ipv6 ospf authentication keychain
- ipv6 policy route-map
- keychain
- key-id
- legacy-inline-power (interface)
- l2protocol dot1q-tunnel
- l2protocol dot1q-tunnel cos
- l2protocol dot1q-tunnel drop-threshold
- l2protocol dot1q-tunnel-mac
- l2protocol dot1q-tunnel shutdown-threshold
- password
- proposal (ipsec)
- rear-module
- reverse-manifest-enable
- send-lifetime
- show dot1x sessions detail
- show hardware nexthop usage
- show keychain
- show l2protocol dot1q-tunnel
- show mac-authentication sessions detail
- show ip ssh rekey statistics
- show rear-module
- spanning-tree path-cost-method
- system-max pms-global-pool
- terminal logging
- tolerance
- tunnel
- tunnel destination
- tunnel protection ipsec
- tunnel source

## Modified commands

The following commands have been modified for this release:

- age
- area virtual-link (OSPFv2)
- clear access-list accounting

- clear overlay-gateway stats
- dot1x-mka-enable
- enable-mka
- extend vlan add (vxlan)
- inline power
- ip interface loopback (vxlan)
- key-server-priority
- legacy-inline-power
- macsec-cipher-suite
- macsec confidentiality-offset
- macsec frame-validation
- macsec replay-protection
- map vlan (vxlan)
- maximum (Port Security)
- mka-config-group
- option
- overlay-gateway
- pre-shared-key
- priority-flow-control
- priority-flow-control enable
- qos egress-shape-ifg-bytes
- qos ingress-buffer-profile
- qos priority-to-pg
- show access-list accounting
- show default values
- show dot1x-mka config
- show dot1x-mka config-group
- show dot1x-mka sessions
- show dot1x sessions
- show dot1x statistics
- show dot1x ip-acl
- show dot1x configuration
- show ip
- show ip dhcp-client options
- show ip ssh
- show mac-authentication sessions
- show mac-authentication statistics
- show mac-authentication ip-acl
- show mac-authentication configuration
- show overlay-gateway
- show running-config
- show span

- site (vxlan)
- spanning-tree (ethernet, lag)
- type (vxlan)
- violation

## Deprecated commands

The following commands have been deprecated beginning with this release:

- ip ospf auth-change-wait-time
- ip ospf authentication-key
- ip ospf md5-authentication
- ip ospf md5-authentication key-activation-wait-time
- ip ssh key-exchange-method dh-group14-sha1
- priority ignore-8021p (supported on legacy platforms only)

# RFCs and standards

## New RFCs and standards

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

- RFC 5709 - OSPFv2 HMAC-SHA Cryptographic Authentication
- RFC 6506 - Supporting Authentication Trailer for OSPFv3
- RFC 7166 - Supporting Authentication Trailer for OSPFv3
- RFC 7348 - Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks

# MIBs

## New MIBs

The following MIBs are new in this release:

- IPsec MIB

# Other Important Changes

## Change in 08.0.70c

**Improvements to the way a phone connection is identified, so that a voice VLAN (tagged VLAN) can be applied:**

From 08.0.70c onwards, a switch will send the default DSCP (46) and priority (5) values as the switch detects phones via LLDP/CDP, even when the Foundry-Voice-Phone-Config VSA is not present.  This reduces the configuration needed for phones since, in most cases, the Foundry-Voice-Phone-Config VSA need not be configured on the RADIUS server to achieve the desired result.

Additionally, 08.0.70c introduces a way to associate usernames with phones for Mac authentication sessions. Admins can configure the USER-NAME standard attribute for such devices in RADIUS server

profiles, so this attribute is sent to switch in ACCESS-Accept, associating the user-name to the Mac authentication session. This makes it very easy to identify the sessions and debug in case of any problems. The user-name is also used in accounting updates, making device identity in transactions easier to read.

This USER-NAME association carries through to sFlow as well. If sFlow is enabled on the port, all the sFlow samples originating from such MAC addresses are added with USER records with the name as sent by RADIUS server. This makes it easier to identify the flows based on user-name instead of MAC address.

How phone connections were handled between 08.0.30d & 08.0.70b:

The "Foundry-Voice-Phone-Config" Vendor Specific Attribute (VSA-11) was added in 8.0.30d, so that the admins can configure the "Foundry-Voice-Phone-Config" in phone device profiles on RADIUS servers. When the switch receives this VSA, the switch treats the device as a phone and can configure the LLDP/CDP dynamically to advertise DSCP and priority values (default: DSCP=46, priority=5) on that port.  (Note that VSA-11 values from RADIUS override the CLI values.)  The syntax for VSA-11 can be found in the Ruckus FastIron Security Configuration Guide. If the VSA is not returned in the RADIUS response, no DSCP or priority info is provided to the phone via LLDP/CDP.

How phone connections were handled prior to 08.0.30d:

A voice VLAN, priority, DSCP, and other parameters are specified using LLDP-MED configuration on the ICX switch. FastIron software communicates those parameters to the phone so that the voice can go in the voice VLAN.

## New MIBs

The following MIBs are new in this release:

IPsec MIB

# Hardware support

## Supported devices

The following devices are supported in this release:

- ICX 7650 Series (ICX 7650-48P, ICX 7650-48ZP, ICX 7650-48F)

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

## 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

FastIron Release 08.0.70a introduces support for the 40G-QSFP-LR4-INT breakout cable.

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 |
|---|---|---|
| ICX 7150 | mnz10111.bin | SPR08070c.bin/SPS08070c.bin |
| ICX 7250 | spz10111.bin | SPR08070c.bin/SPS08070c.bin |
| ICX 7450 | spz10111.bin | SPR08070c.bin/SPS08070c.bin |
| ICX 7650 | tnu10111.bin | TNR08070c.bin/ TNS08070c.bin |

| ICX 7750 | swz10111.bin | SWR08070c.bin/<br>SWS08070c.bin |
| --- | --- | --- |

## PoE firmware files

The following tables lists the PoE firmware file types supported in all 08.0.70 releases. 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: 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.*

*Note: The PoE circuitry includes a microcontroller pre-programmed at the factory. The software can be loaded as an external file. The initial release of the microcontroller code is still current and does not need to be upgraded. 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 Networks Technical Support.*

POE firmware will auto upgrade to version 2.1.0 fw during the loading of FastIron Release 08.0.70. This auto upgrade of the POE firmware will add approximately 10 minutes to the loading of FastIron Release 08.0.70 on the ICX7150, ICX7250, and ICX7450.

Table 1  PoE firmware files

| Device | Firmware version | File name |
| --- | --- | --- |
| ICX 7150 | 2.1.0 fw | icx7xxx_poe_02.1.0.b002.fw |
| ICX 7250 | 2.1.0 fw | icx7xxx_poe_02.1.0.b002.fw |
| ICX 7450 | 2.1.0 fw | icx7xxx_poe_02.1.0.b002.fw |
| ICX 7650 | 2.1.0 fw | icx7xxx_poe_02.1.0.b002.fw |

# Defects

## Closed with code changes in release 08.0.70c

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 4-September-2018 in 08.0.70c.

| 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 | |
| Technology/ Technology Group | |

| Issue | FI-188268 |
|---|---|
| Symptom | legacy PDs cannot be powered or legacy-inline-power cannot configured for PE units. |
| Condition | legacy PDs cannot be powered or legacy-inline-power cannot configured for individual PE units. |
| Workaround | configure legacy-inline-power at port level for the legacy PDs to get powered. |
| Recovery | configure legacy-inline-power on per port for the legacy PDs to get powered. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| 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 | |
| Technology/ Technology Group | |

| 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 | |
| Technology/ Technology Group | Security - 802.1x Port-based Authentication |

| 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-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 | |
| Technology/ Technology Group | Security - RADIUS |

| Issue | FI-186913 |
|---|---|
| Symptom | This is a new safety feature that minimized outages due to micro flaps. Micro flaps can cause L2 and L3  re convergence , resulting in outages lasting minutes. When Link Dampening is configured , micro flaps are monitored and ignored for the configured period , alarms and logs are raised to monitor the link for micro flaps. |
| Condition | Link Dampening may cause momentary traffic loss, convergence issue and other side effects and should be used only when required |
| Workaround | Link dampening can be configured by the linkdampen CLI |
| Recovery | Link dampening can be removed by the no linkdampen CLI. |
| Probability | Low |
| Found In | |
| Technology/ Technology Group | System - System |

| 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 | |
| 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 & 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 | |
| Technology/ Technology Group | |

| Issue | FI-186390 |
|---|---|
| Symptom | no poe functionality on member unit, when units are reloaded with "reload unit-id 2,3". or new unit is added to a stack. |
| Condition | no poe functionality on member unit, when a member unit is reloaded or when new unit is added to a stack. |
| Workaround | Reload the complete stack. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-186015 |
|---|---|
| Symptom | Flexible Authentication configuration is lost, as auth-default-VLAN gets deleted when last port in the auth-default-VLAN is removed. |
| Condition | When last port gets deleted from auth-default-VLAN, the VLAN is deleted which causes removal of Flexible authentication configuration, as auth-default-VLAN is mandatory for other authentication configuration to be valid. |
| Workaround | Keep at least one port in auth-default-VLAN. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-184313 |
|---|---|
| Symptom | Even though Username is associated with MAC-Addr and sent as attribute from RADIUS server during authentication, that attribute is ignored and not shown in MAC-Auth sessions, sflow sampled packets originated from the MAC address. |
| Condition | MAC-Auth sessions do not show the usernames sent by RADIUS server, only show the MAC address as username |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.80 |
| Technology/ Technology Group | Security - MAC Port-based Authentication |

| 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 | FI 08.0.70 |
| 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 | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-185492 |
|---|---|
| Symptom | Loss of BPDU Tunnel packets and customer network not converge. |
| Condition | BPDU Tunnel and MRP configured together. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.80 |
| Technology/ Technology Group | Layer 2 Switching - QnQ - IEEE 802.1Q |

| Issue | FI-184534 |
|---|---|
| Symptom | DHCP snoop, ARP inspection, ND inspection may not work at times when clients logoff and login back causing connectivity issues |
| Condition | When user logs off, the port is deleted from VLAN, which leads to deletion of DHCP snoop entry. When the user logs back in, as the earlier DHCP acquired address is good to use (lease not expired), snoop, DAI and NDI tables don't get populated again leading to ARP/ND inspection issues. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.80 |
| Technology/ Technology Group | |

| Issue | FI-185177 |
|---|---|
| Symptom | LLDP capable phone is not operational after port is brought down and then up |
| Condition | When port goes down for LLDP capable phones, LLDP shutdown message is not sent, so when the port is back up again, phone thinks the voice session still exists, so session is not attempted by phone. |
| Workaround | At the interface config level, toggle inline-power, so the phone resets after port is up. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - MAC Port-based Authentication |

| Issue | FI-184517 |
|---|---|
| Symptom | Changing auth-timeout-action sometimes causes sessions to be not established, when RADIUS servers are not available |
| Condition | Sessions are not established sometimes as AAA indicates server not available, and the sessions which are re-authenticating or authenticating are cleared. Instead apply the timeout-action when servers are not available and avoid clearing the sessions |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - MAC Port-based Authentication |

| Issue | FI-183578 |
|---|---|
| Symptom | Vulnerability : CVE-2018-7185<br>Denial of Service attack causing the victim Network Time Protocol daemon (ntpd) to reset its association. |
| Condition | Vulnerability : CVE-2018-7185<br>Denial of Service attack causing the victim Network Time Protocol daemon (ntpd) to reset its association. |
| Workaround | None |
| Recovery | None |
| Probability | Low |
| Found In | FI 08.0.80 |
| Technology/ Technology Group | Management - NTP - Network Time Protocol |

| Issue | FI-182671 |
|---|---|
| Symptom | Loss of BPDU Tunnel packets and customer network not converge. |
| Condition | BPDU Tunnel feature enabled, with rate limit configured on a port or LAG. |
| Workaround | None |
| Recovery | Remove BPDU Tunnel rate limit configuration on the port or LAG. |
| Probability | Medium |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Layer 2 Switching - QnQ - IEEE 802.1Q |

| Issue | FI-188315 |
|---|---|
| Symptom | Support save was issued more than once. Core file was deleted during the first execution of support save . Due to this SS size gets reduced during the subsequent execution. |
| Condition | Core file gets deleted when support save was not completed successfully. Fix is provided to retain core files in cases where support save is not successful. On successful completion of support save core file will get deleted. So customer should provide first successful support save out for debugging. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | |
| 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 | |
| Technology/ Technology Group | Management - PoE/PoE+ - Power over Ethernet |

| 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.<br>1. A vlan without any ports is configured as auth-default-vlan and few ports are configured for Flexauth.<br>2. Configuration is saved and reloaded.<br>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 | |
| Technology/ Technology Group | Security - MAC Port-based Authentication |

| Issue | FI-187404 |
|---|---|
| Symptom | "SysobjectID" returns value of '0' with model 7150-48ZP. |
| Condition | SNMP get of " .1.3.6.1.2.1.1.2.0" for SysobjectID returns 0 on 7150-48ZP |
| Workaround | N/A |
| Recovery | N/A |
| Probability | High |
| Found In | |
| Technology/ Technology Group | Management - SNMP - Simple Network Management Protocol |

| Issue | FI-187170 |
|---|---|
| Symptom | Crash due to memory leak "no logging buffered debugging" is configured. |
| Condition | Device crash due to memory leak when "no logging buffered debugging" |
| Workaround | Remove no logging buffered debugging from configuration as a Workaround |
| Recovery | N/A |
| Probability | Low |
| Found In | |
| Technology/ Technology Group | Monitoring - sFlow |

| Issue | FI-186670 |
|---|---|
| Symptom | This issue happens very rarely and it is a corner case. In this case the port state mismatch is observed between stacking Active and the Standby where the Active shows port status as Down and Standby port status is shown as Up |
| Condition | This issue happens in a very rare case when PD device is connected to the ICX7450 POE port on the stacking standby unit after the stack reload is performed. |
| Workaround | None |
| Recovery | Recovery procedure is to reload the particular stacking unit or the entire stack |
| Probability | Medium |
| Found In | |
| Technology/ Technology Group | Management - PoE/PoE+ |

| 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 | |
| Technology/ Technology Group | System - System |

| Issue | FI-184784 |
|---|---|
| Symptom | Issue seem to be appeared during stack merge. |
| Condition | config sync event during the stack merge scenario caused the invalid memory access which leads to crash |
| Workaround | None |
| Recovery | None |
| Probability | Medium |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | System - System |

| Issue | FI-184262 |
|---|---|
| Symptom | Rconsole from active unit hangs to member unit of the stack |
| Condition | Rconsole to the member unit of the stack, the console session gets hung |
| Workaround | None |
| Recovery | Rcosole 2 never completes, it hangs, they have to kill the connection to recover |
| Probability | Low |
| Found In | FI 08.0.70 |
| Technology/ Technology | Stacking - Stack Management |

| Group | |
|---|---|

| Issue | FI-182320 |
|---|---|
| Symptom | On ICX device, interface added as tagged or untagged to non default-vlan still shows as untagged to default vlan |
| Condition | When interface belongs/untagged to default vlan is untagged or tagged to some other vlan then the interface should not be shown as part of default-vlan |
| Workaround | No functional impact. |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Layer 2 Switching - VLAN - Virtual LAN |

| Issue | FI-187525 |
|---|---|
| Symptom | After upgrading the ICX device, radius-server configuration gets automatically appended with mac-auth, dot1x and webauth keyword, when the keywords are actually not configured for the command. |
| Condition | ICX device is upgraded to latest release. Radius-server command is configured without mac-auth, dot1x and webauth keywords. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | |
| Technology/ Technology Group | |

| Issue | FI-186852 |
|---|---|
| Symptom | PoE functionality on some ports will not be available when device(PoE Chip) fails during operation. These ports will show up as software problem or internal h/w fault in the show inline power command output. A reboot will cause switch to boot without PoE function on the unit (all ports). |
| Condition | This issue will be seen when PoE chip on the ICX device fails |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | |
| Technology/ Technology Group | |

| Issue | FI-186762 |
|---|---|
| Symptom | ifNumber object would display wrong value |
| Condition | snmp walk of ifNumber interface Mib would include maximum supported LAG interfaces too. |
| Workaround | NA |
| Recovery | NA |
| Probability | |
| Found In | |
| Technology/ Technology Group | |

| 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.<br>2. Ping from one device to the other device. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | |
| Technology/ Technology Group | |

| 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.<br>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.<br><br>"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 | |
| Found In | |
| Technology/ Technology Group | |

| Issue | FI-185991 |
|---|---|
| Symptom | 'Broadcast limit', 'multicast limit' and 'unknown-unicast limit' configurations are accepted on PE ports but they do not work. |
| Condition | 'Broadcast limit', 'multicast limit' or 'unknown-unicast limit' are configured on PE port. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | |
| Technology/ Technology Group | |

| Issue | FI-186388 |
|---|---|
| Symptom | After active unit resets and it comes back up and becomes active again, IPv4 routed traffic ingress on standby unit's ports are trapped to active CPU instead of hardware forwarding causing high CPU on active. |
| Condition | During Active/Standby synchronization of ARP/IP Cache table if switchover happens during that time the problem could be seen, thus it a corner case timing problem. It could happens with the following conditions:<br>1: the setup is scaled SPX or Stacking setup, (seen on SPX with 29 PE)<br>2: Active unit has higher priority than standby unit<br>3: arp table and ip cache table size is more than 1000,<br>4: Active unit Resets and comes back up and it automatically switch-over to active. |
| Workaround | Reduce the Priority of Active to be same as Standby, and if required after active resets and comes back up as Standby. Wait till on new Active message "[L3 UCAST HITLESS FAILOVER]: IPv4 Unicast hitless failover completed" is printed, then do switch over manually to make Standby becomes Active again. |
| Recovery | In the problem state "clear arp" on active unit can solve the issue and traffic will do hardware forwarding after re-learning of ARP. |
| Probability | |
| Found In | |
| Technology/ Technology Group | Layer 3 Routing/Network Layer - ARP - Address Resolution Protocol |

| Issue | FI-185997 |
|---|---|
| Symptom | Command link-error-disable doesn't work on  lag ports |
| Condition | "link-error-disable " doesn't work on a  lag port . |
| Workaround | N/A |
| Recovery | N/A |
| Probability | High |
| Found In | |
| Technology/ Technology Group | |

| 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-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 | |
| 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-109837 |
|---|---|
| Symptom | SSH configuration with ACLs on the SSH access group is not working. |
| Condition | 1. Change ssh port number: ip ssh port <xxx><br>2. Configure access list: access-list <y> permit any<br>3. Configure access list on ssh: ssh access-group <y><br>4. wr mem and reload |
| Workaround | |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.30 |
| Technology/<br>Technology<br>Group | Management - Configuration Fundamentals |

| Issue | FI-183943 |
|---|---|
| Symptom | Authentication, Authorization and Accounting of login feature like telnet, SSH, EXEC stops working after few login and logouts. |
| Condition | AAA is enabled for login features like telnet, SSH and EXEC. |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.30 |

| Issue | FI-183100 |
|---|---|
| Symptom | System resets rarely while connecting third party network monitoring tool with ICX device. |
| Condition | More number of HTTP, HTTPS, SSL requests polling the web management module, leads to system reset. |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.70 |
| Technology/<br>Technology<br>Group | |

| Issue | FI-184089 |
|---|---|
| Symptom | Switch reloads on executing a batch buffer script on a stack setup. |
| Condition | A reload is triggered by executing a batch buffer script on a stack setup when the script execution leaves the CLI prompt in any mode other than PRIVILEGED EXEC mode |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.70 |
| Technology/<br>Technology<br>Group | Management - CLI - Command Line Interface |

| Issue | FI-184066 |
|---|---|
| Symptom | When IP ACL and DSCP remark commands are configured on an interface, after reload, ip traffic other than ICMP is blocked by the interface. |
| Condition | IP-ACL and DSCP remark commands are configured on an ve interface then traffic is blocked after reload due to wrong programming. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-183203 |
|---|---|
| Symptom | The RX_Power value obtained from mib browser and by running show optic command is different |
| Condition | Verify the show optic for that particular interface from cli and from mib browser. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| 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 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-182302 |
|---|---|
| Symptom | Although destination MAC address is correctly learned, traffic is getting flooded out on multiple ports. |
| Condition | When the stacking port goes down, ACL unbind is called where the port bit mask is updated for all the rules on that port. |
| Workaround | None |
| Recovery | None |
| Probability | Low |
| Found In | FI 08.0.61 |

| 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 | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-182608 |
|---|---|
| Symptom | ICX device might unexpectedly reload when the last port is removed from a LAG |
| Condition | Remove the last port from the LAG |
| Workaround | None |
| Recovery | None |
| Probability | Low |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-182248 |
|---|---|
| Symptom | Traffic from/to clients in non-default-VLAN 1 with VRF is dropped at ICX device. |
| Condition | VLAN different from VLAN 1 is configured as system-default-VLAN. VLAN 1 is created as a layer 3 VLAN with VRF. A reload has been performed on the stack. |
| Workaround | |
| Recovery | |
| Probability | High |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | |

# Closed with code changes in release 08.0.70b

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 6-April-2018 in 08.0.70b.

| Issue | FI-180346 |
|---|---|
| Symptom | Unexpected reload happen on unit 1 of 4 unit stack. |
| Condition | On ICX stack while processing IPC message on stack unit, reload happens on one of the units due to invalid memory access. |
| Workaround | |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.40 |
| Technology/ Technology Group | System - System |

| Issue | FI-181963 |
|---|---|
| Symptom | Configured max-reauth request value is not updated in show dot1x configuration |
| Condition | On ICX devices, it always shows default value for max-reauth request in show dot1x configuration even though user change it to a different value. |
| Workaround | No functional impact |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Management - CLI - Command Line Interface |

| Issue | FI-180553 |
|---|---|
| Symptom | PoE powersupply is shown as regular powersupply during bootup in active unit. |
| Condition | Issue can be seen while executing the below set of commands. 1.clear syslog 2. reload the device 3. show log |
| Workaround | No Workaround |
| Recovery | None. |
| Probability | Low |
| Found In | FI 08.0.30 |
| Technology/ | Monitoring - Syslog |

| Technology Group | |
|---|---|
| | |

| Issue | FI-181825 |
|---|---|
| Symptom | Continuous reload seen when adding a new unit to the stack. |
| Condition | 1."urpf" configured on the stack with "system-max ip-route/system-max ip6-route" set to a non-default value on the stack.<br>2.New unit with no running config is added to the stack.<br>3.New unit gets into continuous reload. |
| Workaround | NA |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Stacking - Secure Setup, Autoconfig, Manifest files, Autocopy |

| Issue | FI-181728 |
|---|---|
| Symptom | When stp-bpdu's are received, the interface will move to Up and Disabled state. |
| Condition | In ICX7250 enable stp-bpdu-guard in the interface level and when stp-bpdu's are received. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Layer 2 Switching - BPDU Guard - Bridge Protocol Data Unit |

| Issue | FI-181448 |
|---|---|
| Symptom | linkDown snmp trap contains unexpected value |
| Condition | On ICX devices, when operationally enabled port is disabled then operational status will be shown in snmp TRAP on mib browser as "Up" always. Issue seen only with snmp trap. |
| Workaround | No functional impact. |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Management - SNMP - Simple Network Management Protocol |

| Issue | FI-180474 |
|---|---|
| Symptom | Switch might reload while processing FDP packets. |
| Condition | Switch might reload while processing FDP packets. |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 07.4.00 |
| Technology/ Technology Group | Management - FDP - Foundry Discovery Protocol |

| Issue | FI-181529 |
|---|---|
| Symptom | Sflow collector reports XDR error. |
| Condition | 802.1x authentication and sflow are enabled on the same interface. Sflow sends user-name attribute in the sample packet. |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Security |

| Issue | FI-181537 |
|---|---|
| Symptom | show clock detail shows summer time start and end date incorrectly. |
| Condition | configure "clock summer-time" and "clock timezone us Eastern". show clock details displays incorrect start and end date for summer time |
| Workaround | NA |
| Recovery | NA |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Management - CLI - Command Line Interface |

| 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 | |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Security - RADIUS |

| Issue | FI-181565 |
|---|---|
| Symptom | On ICX7650, if the stacking trunk is configured, and trying to do unit replacement on standby unit, could causes the protocols packet not reaching the standby unit. |
| Condition | This issue is observed only when stacking trunk is configured and unit replacement is done for the standby unit. |
| Workaround | None |
| Recovery | Reload the standby unit will recover from this condition |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | IP Multicast - IGMP - Internet Group Management Protocol |

| Issue | FI-181683 |
|---|---|
| Symptom | When support save all (display or tftp) command is executed, CPU spikes to 99% and data traffic is dropped |
| Condition | On ICX7XXX devices, supportsave all display command is triggered when flexauth dot1x is enabled. |
| Workaround | removing flexauth config will not create any issue in supportsave display. But this is not possible workaround for all customers. |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Management - Configuration Fundamentals |

| Issue | FI-182899 |
|---|---|
| Symptom | Security vulnerability in web server due to a script. |
| Condition | Security vulnerability in web server due to a script. |
| Workaround | |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Security - Security Vulnerability |

| Issue | FI-180143 |
|---|---|
| Symptom | Unexpected reload seen in ICX stack of 1 unit |
| Condition | On ICX devices while trying to print buffer in console, reload occurs due to negative length value. |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Management |

| Issue | FI-182122 |
|---|---|
| Symptom | During Dhcp Atuo Provisioning While applying the configuration downloaded from TFTP server the remark configuration done for ACL's will be overwritten . |
| Condition | DHCP auto provisioning should be used to load the running configuration with multiple ACL's having remarks . |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-182212 |
|---|---|
| Symptom | On ICX7750 stack when polled for temperature values for all the units remote units temperature will be shown as 0. |
| Condition | Issue is seen with ICX7750 stack when polled for temperature of remote units . |
| Workaround | None |
| Recovery | |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Management - SNMP - Simple Network Management Protocol |

| Issue | FI-183753 |
|---|---|
| Symptom | When reauth period and session timeout sent from RADIUS server are same values (which is generally not same, as reauth-period tend to be high and session-timeout small), 2 reauth attempts are made for the session which triggers the reauth failure from RADIUS client on the switch. |
| Condition | Reauth time |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - MAC Port-based Authentication |

| Issue | FI-182196 |
|---|---|
| Symptom | When MAC-Auth succeeds and returns U:x, T:y, 2 sessions are opened with one each for Untagged and tagged VLANs (the trigger is sending tagged packets from client).  Later when VLAN movement happens for updating the untagged session, the tagged VLAN session also gets updated with untagged VLAN. On subsequent receipt of tagged packets from same client, another tagged session gets created (duplicate). |
| Condition | Any MAC Authentication time |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - MAC Port-based Authentication |

| Issue | FI-183370 |
|---|---|
| Symptom | When a session is cleared, some times an MBV (MAC-VLAN table) entry is  left behind. With such entries, the incoming packets get classified in the VLAN identified by MBV entry and port may have been removed from that VLAN earlier. The VLAN membership check fails for new authentication triggers, which is not required, so the check is removed. |
| Condition | Reauth time |
| Workaround | |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - 802.1x Port-based Authentication |

| Issue | FI-183964 |
|---|---|
| Symptom | When 802.1X enable flag is changed from 0 to 1 during reauthentication, the session gets cleared on the local units where the session are originated from. As the control is changed from MAC-Auth to 802.1X, the session removal on the ACTIVE unit doesn't happen, which leaves the session entry. When subsequent packets hit the ACTIVE unit for MAC-Auth, as the session exists, authentication is not performed and MAC is learnt in the FDB tables. |
| Condition | Reauth time |
| Workaround | |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - 802.1x Port-based Authentication |

| Issue | FI-181265 |
|---|---|
| Symptom | Unexpected reboot of unit 4 in a stack due to sflow packets. |
| Condition | 4-unit stack with sflow enabled. |
| Workaround | NA |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Stacking - Traditional Stacking |

| Issue | FI-181254 |
|---|---|
| Symptom | CPU spike is caused by 239.255.255.250 groups. Applying an ACL to block these groups is not working on route-only port when PIM flaps. |
| Condition | ACL cannot block the mcache creation because mcache entry is created using PIM join . |
| Workaround | |
| Recovery | Configure the ACL in FHR, LHR |
| Probability | |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-182229 |
|---|---|
| Symptom | snmp bulkwalk gives incorrect value for bgp4V2PeerDescription. |
| Condition | 1.configure snmp-server. 2.Establish BGP connection with 4-5peers. 3.Try snmpwalk and snmpbulkwalk of bgp4V2PeerDescription. snmpbulkwalk values will be incorrect. |
| Workaround | NA |
| Recovery | |
| Probability | Low |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Management - SNMP - Simple Network Management Protocol |

| Issue | FI-182031 |
|---|---|
| Symptom | Scheduled reset from secondary in a stack boots from primary. |
| Condition | reload at <time> from <secondary> cli command boots from primary in a stack. |
| Workaround | NA |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Stacking - Traditional Stacking |

| Issue | FI-183466 |
|---|---|
| Symptom | "Error: MAX-Session is Reached" is displayed and User stays in vlan 4092 |
| Condition | 802.1x-Enable attribute is changed for a phone by Server during mac-auth<br>re-authentication. If this attribute keep changing between 0 & 1 during re-authentication, "Error: MAX-Session is Reached" is displayed and phone is unable to join the network |
| Workaround | Donot change the 802.1x-Enable attribute after mac-authentication is completed |
| Recovery | Bounce the port |
| Probability | High |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - 802.1x Port-based Authentication |

| Issue | FI-183794 |
|---|---|
| Symptom | The RADIUS servers are classified as down on ACTIVE unit, though they are up, whereas they are classified as up on all other units in the stack. This continues until the dead radius interval expires first time, at which time, it gets fixed. |
| Condition | On reload |
| Workaround | |
| Recovery | |
| Probability | High |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - MAC Port-based Authentication |

## Closed with code changes in release 08.0.70a

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 19-January-2018 in 08.0.70a.

| Issue | FI-181734 |
|---|---|
| Symptom | Continuous reload seen when adding a new unit to the stack. |
| Condition | 1."system-max ip-arp" set to a non-default value on the stack.<br>2.New unit with no running config is added to the stack.<br>3.New unit gets into continuous reload. |
| Workaround | NA |
| Recovery | Whenever a new value for "system-max ip-arp" is set, the ICX device must be reloaded for the configuration to take effect. |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | System/System |

| Issue | FI-181239 |
|---|---|
| Symptom | DHCP clients such as SONOS speakers, Ring cameras, EcoBee3 devices are not getting IP address from ICX. |
| Condition | When ICX device is used as DHCP server, the DHCP clients such as SONOS speakers, Ring cameras, EcoBee3 are not able to get IP address. |
| Workaround | None |
| Recovery | None |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Management/DHCP |

| Issue | FI-181681 |
|---|---|
| Symptom | User was not able do mac-authentication |
| Condition | When Flexauth port is disabled and then enabled again |
| Workaround | None |
| Recovery | Reload the Stack |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Security - MAC Port-based Authentication |

| Issue | FI-181812 |
|---|---|
| Symptom | The Dot1x client PC stays in "CONNECTING" state and not getting authenticated. |
| Condition | When the Dot1x client PC goes to sleep mode and comes back, it is not authenticated and so stays in the "CONNECTING" state. |
| Workaround | None |
| Recovery | None |
| Probability | Medium |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - 802.1x Port-based Authentication |

| Issue | FI-181611 |
|---|---|
| Symptom | 'Session-Timeout' attribute is not updating the re-authentication period for the 802.1x authenticated User |
| Condition | When 'Session-Timeout' attribute is sent by Radius-Server for an 802.1x authenticated User |
| Workaround | Set the 'Session-Timeout' value to re-auth period from CLI |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - 802.1x Port-based Authentication |

| Issue | FI-181570 |
|---|---|
| Symptom | While the user is authenticated, modification of ACL through CoA fails and if the port happens to be on standby unit, the old ACL filters are still in effect and new ACL filters are not programmed leading to unintended data transfer through switch. |
| Condition | When CoA is performed from external AAA server for an existing WebAuth session to modify the existing ACL with a new ACL |
| Workaround | Using CoA, disconnect the session, so the user when authenticated next time gets the new ACL configured on the AAA server. Other way is to clear or reset the session on the switch, so the authentication gets triggered again and new ACL will be applied |
| Recovery | Using CoA, disconnect the session, so the user when authenticated next time gets the new ACL configured on the AAA server. Other way is to clear or reset the session on the switch, so the authentication gets triggered again and new ACL will be applied |
| Probability | Medium |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - Web Authentication |

| Issue | FI-181508 |
|---|---|
| Symptom | When multiple telnet sessions are opened and multiple configuration download operations are done, system can go into a state where it continuously prints "Failed to open gpio value for reading". |
| Condition | When multiple telnet sessions are opened and multiple configuration download operations are done, system can continuously print "Failed to open gpio value for reading". |
| Workaround | Do not run multiple configuration downloads from multiple telnet sessions simultaneously . |
| Recovery | Reload the system to recover from this state. |
| Probability | High |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Management - IPv4/IPv6 Host Management |

| Issue | FI-177595 |
|---|---|
| Symptom | In rare circumstances, when ICX7650 boots up, a hardware initialization failure could trigger an additional reboot with the following error message - "FATAL ERROR: Failed in HW init hence rebooting". |
| Condition | In rare circumstances, when ICX7650 boots up, a hardware initialisation failure could trigger additional reboots. In this defect scenario, initialisation of 10GF port fails. |
| Workaround | No workaround available. |
| Recovery | No recovery needed. System recovers from the hardware initialization failure by rebooting automatically. |

| Probability | Medium |
|---|---|
| Found In | FI 08.0.70 |
| Technology/ Technology Group | System/System |

## Known issues in release 08.0.70a

This section lists open software defects with Critical, High, and Medium Technical Severity as of 19-January-2018 in 08.0.70a.

| Issue | FI-182092 |
|---|---|
| Symptom | When 40G-QSFP-LR4-INT breakout cable is inserted, the neighbouring port LEDs lit up green. |
| Condition | The issue is seen when 40G-QSFP-LR4-INT breakout cable is inserted. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.70 |
| Technology/Technology Group | System - Optics |

## Closed with code changes in release 08.0.70

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of December 21, 2017 in 08.0.70.

| Issue | FI-181317 |
|---|---|
| Symptom | router can crash when using multi-spx-lag. |
| Condition | use the CLI multi-spx-lag to config the lag |
| Workaround | none |
| Recovery | don't use the multi-spx-lag |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181143 |
|---|---|
| Symptom | "show mac-addr" shows "0000.0000.0000" entry in MCT configuration. |
| Condition | When system has MCT configured and system is learning MAC addresses, this problem may be exposed occasionally due to MAC hash collisions.. |
| Workaround | . |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ | |

| Technology<br>Group | |
|---|---|

| **Issue** | **FI-181066** |
|---|---|
| Symptom | In FIPS mode, show running config, displays keys in plain text for MKA protocols instead of masked keys "...." |
| Condition | FIPS mode should be enabled.<br>MKA keys should be configured. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/<br>Technology<br>Group | |

| **Issue** | **FI-180967** |
|---|---|
| Symptom | IP Source-guard feature is not working on Port Extender (PE) ports after a reload of the PE unit or reload of the entire SPX stack |
| Condition | IP Source-guard is configured on Port Extender (PE) ports through VLAN. VLAN is not configured with Virtual VE ports<br>PE unit is reloaded (PE unit alone or all units of the stack) |
| Workaround | Remove the IP Source-guard config on PE port and re-apply |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/<br>Technology<br>Group | |

| **Issue** | **FI-180695** |
|---|---|
| Symptom | In FIPS mode, for MKA keys, the keys were masked off, only if the pre-shared-key started with 0, 1 or 2.<br><br>If the keys started with rest of the hex digits, that is from 3 to F, it showed plain text keys. |
| Condition | FIPS mode should be enabled.<br>MKA pre-shared-keys should be configured with starting hex digit other 0, 1 or 2. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/<br>Technology<br>Group | |

| Issue | FI-180677 |
|---|---|
| Symptom | we don't support different speed on the spx lag. speed change should be blocked on spx lag |
| Condition | changing speed on different interface in the lag is not supported. |
| Workaround | don't change speed on the lag |
| Recovery | make sure the speed is the same on all the interface before adding to the spx lag. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180117 |
|---|---|
| Symptom | Unexpected reload of stacking happens when stacking was enabled. |
| Condition | When the stacking was enabled, memory was corrupted which lead to multiple iterations of a while loop and triggered the watchdog timeout. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | |

| Issue | FI-180583 |
|---|---|
| Symptom | CPU is not receiving control packet on the protocol. Stack break. |
| Condition | CPU is not receiving control packet on the protocol. Stack break. |
| Workaround | Reload the system |
| Recovery | Reload the system |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180472 |
|---|---|
| Symptom | When user removes the last port from the vlan, IPv6 and IPv4 Ingress ACL associated with that vlan's router interface are not getting cleaned up in the TCAM though the ACL configuration on the Router Interface (VE) is removed implicitly by the system. Traffic will be subjected to the ACL filtering if the port is added back to the vlan. |
| Condition | User will encounter this issue when<br>1. An IPv4 or IPv6 ACL is bound on a virtual interface of a vlan<br>2. There is only one port in the vlan<br>3. User removes this last port from the Vlan |
| Workaround | The user can remove the IPv4 and IPv6 ACL from the Router Interface (VE) before removing the last port from the Vlan to avoid running into this issue. |
| Recovery | The user should reload the stack units corresponding to the last port removed from the Vlan. In case VLAG is the last member removed from the Vlan, user should reload all the stack units corresponding to members of the VLAG. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180348 |
|---|---|
| Symptom | protocol flaps and stack break |
| Condition | when there is a lot of traffic sent to CPU, CPU Rx can get stuck. |
| Workaround | reload the units to recover |
| Recovery | reload the units to recover |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-121550 |
|---|---|
| Symptom | When "snmp-server enable traps mac-notification" configuration is disabled, the syslog "MAC-Event: MAC:0000.0000.0000-VLAN:0-PORT:1/1/19-ACT:4::" is generated. |
| Condition | The command "snmp-server enable traps mac-notification" is configured and the user is trying to disable the command. |
| Workaround | |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | |

| Issue | FI-180049 |
|---|---|

| Symptom | Inline power configuration not listing the class-4 option in ICX WEB user interface |
|---|---|
| Condition | On the "Configure Inline Power" page for the ICX Web GUI, after selecting the "Allocate power by class" radio button, when the "Power by class" drop-down menu is clicked, the "Class-4" option is not listed. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-179364 |
|---|---|
| Symptom | After reload, IPSG configuration on LAG under VLAN is missing |
| Condition | Have IPSG on Physical interface and on LAG under same VLAN. Write configuration to memory and reload unit. After reload, IPSG config on VLAG under VLAN is missing. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Security - IP Source Guard |

| Issue | FI-179997 |
|---|---|
| Symptom | ICX device unexpectedly reloads while walking the IP MIB |
| Condition | The issue is only seen when walking the IP MIB using the SilverCreek tool. Other mechanisms for walking the IP MIB do not trigger the unexpected reload. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-176154 |
|---|---|
| Symptom | On ICX7450 system when user issues the command "show cpu task" to know the CPU utilization data then sometime the CPU utilization is shown incorrectly as 0% for the application task |
| Condition | This issue happens on ICX7450 switch when user issues the command "show cpu task" to know the CPU utilization for different tasks |

| Workaround | The high level command "show cpu" works fine and displays overall cpu utilization without task level granularity |
|---|---|
| Recovery | |
| Probability | |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Management - CLI - Command Line Interface |

| Issue | **FI-179698** |
|---|---|
| Symptom | Some ports doesn't release power reservation in a special case where all class 4 PDs are connected at a single shot and each of the PDs are consuming maximum power of 25.5W. |
| Condition | "show inline power" output is not accurate as the port says there is some power allocated while the port is actually disabled because of power budget. |
| Workaround | None |
| Recovery | configure the port with "no inline power" and then "inline power" to get the port back to proper state. |
| Probability | |
| Found In | FI 08.0.70 |

| Issue | **FI-179696** |
|---|---|
| Symptom | ICX device unexpectedly reloads while performing set operation for USM-MIB(RFC-3414) using SNMPv3. |
| Condition | This issue is seen when performing set operation for USM-MIB(RFC-3414) using the SilverCreek tool with SNMPv3 configured. Other mechanisms for set operation of the USM-MIB(RFC-3414) do not trigger the unexpected reload. When other versions of SNMP are used, the issue is not seen. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | **FI-179536** |
|---|---|
| Symptom | Removing a vlan configuration is not removing IP Source-guard configuration enabled on the VLAN |
| Condition | 1. IP Source-guard is configured on all ports of a VLAN. 2. Remove VLAN configuration is removed from the switch. 3. Configuring the same VLAN will lead to re-configuring of IP Source-guard feature |
| Workaround | Remove the IP Source-guard feature from the VLAN before removing it |
| Recovery | None |
| Probability | |

| Found In | FI 08.0.70 |
|---|---|
| Technology/ Technology Group | Security - IP Source Guard |

| **Issue** | **FI-179374** |
|---|---|
| Symptom | With the campus fabric topology, ICX7750 standby control bridge encounters unexpected unit reload during the ring topology formation with the port extenders. |
| Condition | This issue is observed in rare case during the ring topology formation with the port extenders. |
| Workaround | None |
| Recovery | Standby control bridge will automatically recover after the unit reload |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| **Issue** | **FI-179372** |
|---|---|
| Symptom | Removing a LAG configuration and re-creating the same LAG fails when IP Source-guard is enabled on the LAG interface. Below error message is thrown while re-creating it "Lag Ap Add Failed( Critical Error )" |
| Condition | LAG interface is created and IP Source-guard is configured on the LAG interface. Delete the LAG interface and re-create the same LAG interface |
| Workaround | Remove IP Source-guard configuration before deleting the LAG interface. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - IP Source Guard |

| Issue | FI-179356 |
|---|---|
| Symptom | IP Source-guard Static entries are not allowed to be configured and below error is thrown when user deletes and re-creates the same LAG and IPSG is enabled on the LAG<br>Switch(config)#ip source bind 192.85.1.107 lag 1 vlan 1<br>Warning - IP Source Guard is Not configured on the per-port-per-vlan 1 for port lg1, 192.85.1.107 binding will not be active. |
| Condition | 1. LAG interface is created and added to a VLAN<br>2. IP Source-guard is enabled on the VLAN<br>3. LAG interface is deleted.<br>4. Same LAG interface is created.<br>5. User tries to create IPSG Static entry on the LAG interface |
| Workaround | Disable IP Source-guard on the VLAN before deleting the LAG interface in step 3 above |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - IP Source Guard |

| Issue | FI-179332 |
|---|---|
| Symptom | ACL Accounting counters are not incrementing for Stack Member unit ports on which IPv4 or IPv6 ACL (with Accounting enabled) is configured |
| Condition | IPv4 ACL or IPv6 ACL with Accounting enabled on the ACL is applied on a Stack Member unit's Port.<br>Same ACL is applied on two ports of the same Stack Member unit<br>One Port has Logging enabled and the other without Logging. |
| Workaround | Have Logging enabled/disabled on both the ports of the Stack Member unit |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-179190 |
|---|---|
| Symptom | The supportsave operation fails when it was initiated with incorrect server address followed by correct server. Even though in the second attempt correct server address was provided it doesn't work. |
| Condition | When "supportsave core" operation was initiated with wrong/unreachable tftp server once which will fail, later even after giving correct/reachable server doesn't work forever, till ICX is reloaded to recover from this state. |
| Workaround | None |
| Recovery | Reload the ICX to recover from this error state |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | None - None |

| Issue | FI-179116 |
|---|---|
| Symptom | ICX device unexpectedly reloads while performing set operation for USM-MIB(RFC-3414) using SNMPv3. |
| Condition | This issue is seen when performing set operation for USM-MIB(RFC-3414) using the SilverCreek tool with SNMPv3 configured. Other mechanisms for set operation of the USM-MIB(RFC-3414) do not trigger the unexpected reload. When other versions of SNMP are used, the issue is not seen. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-179000 |
|---|---|
| Symptom | IP Multicast traffic may be observed on some interfaces/ports that were not part of that multicast group. |
| Condition | Changing default vlan sometime create this problem on a system. This problem is applicable to all Products and all releases prior to 8070. |
| Workaround | |
| Recovery | Clear ip pim mcache <source group address> |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | IP Multicast - PIM - Protocol-Independent Multicast |

| Issue | FI-178936 |
|---|---|
| Symptom | Error message is displayed to the user like the one below when trying to remove a configured security feature(Example: IPv4/IPv6 acl ,DSCP) from router interface, even though internally the respective security feature is removed from the router interface.<br>"Error : Unable to remove the binding of the V6 ACL scale22 from interface v646."<br><br>Also, further configuration of IPv4/IPv6 acl to the same router interface will result in the following error and the operation also does not succeed. "Insufficient hardware resources to apply the ACL. Please remove already applied ACL(s) and/or Security features and try again." |
| Condition | This issue will be seen with the following sequence of steps:<br>1. Ports from the same stack member unit are part of 2 different vlans.<br>2. Same security feature(Example: DSCP,IPv4 acl) is configured on the router interface of both the vlans.<br>3.One of the router interfaces has an additional security feature(Example: ipv6 acl) configured.<br>4. acl-per-port-per-vlan configuration is not enabled.<br>5. Remove the additional configured feature (IPv6 acl) on one of the router interfaces. |
| Workaround | User can use the following steps when removing the additional security feature to avoid running into this issue.<br>Step 1: Remove all the common security features configured among these router interfaces first.<br>Step 2:  Remove the intended security feature.<br>Step 3: Re-configure the common security features removed in step 1. |
| Recovery | Reloading the stack member unit will recover from this issue. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-178844 |
|---|---|
| Symptom | TP counters for standby ports don't work. |
| Condition | 1. TP must be installed on standby ports.<br>2. There should be a matching traffic for the same. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-178698 |
|---|---|
| Symptom | ACL Accounting Counters are not incremented on enabling and disabling Accounting at the ACL level. |
| Condition | IPv4 or IPv6 ACL with Accounting enabled is applied on an interface. ACL has multiple Port Range (UDP or TCP Port Range) based filters. ACL Accounting is disabled and enabled. At this time, Accounting Counters stops incrementing |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-178686 |
|---|---|
| Symptom | Ping failure to /32 IP Address of a loopback interface. |
| Condition | When an already configured static host route prefix is configured as a loopback interface IP. Then, ping to that loopback interface IP Address fails. |
| Workaround | Removing the static route and then configure the loopback interface IP Address |
| Recovery | Disable and enable the loopback interface would make the ping work. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Layer 3 Routing/Network Layer - IP Addressing |

| Issue | FI-169096 |
|---|---|
| Symptom | In ICX devices, GRE keepalive tunnel doesn't come up after the intermediate device link went down. |
| Condition | In ICX devices, when an intermediate device link goes down, it causes the GRE keepalive to be marked down due to keepalive packets not flowing. |
| Workaround | |
| Recovery | GRE keepalive tunnel can be recovered by manually disable and enable of the GRE tunnel |
| Probability | |
| Found In | FI 08.0.60 |
| Technology/ Technology Group | Layer 3 Routing/Network Layer - GRE - Generic Routing Encapsulation |

| Issue | FI-178511 |
|---|---|
| Symptom | When a physical port is removed from LAG, IP Source-guard entries learnt on the port is not updated |
| Condition | A physical port is added to a LAG Interface and the LAG is added to a VLAN<br>DHCP Snooping and IP Source-guard is enabled on the VLAN<br>DHCP client gets an IP over the LAG Interface and DHCP Snooping table is populated with those entries. IP Source-guard Table is also updated.<br>Physical port is removed from the LAG interface<br>DHCP Snooping table shows the entry against the Physical port, but IP Source-guard table shows the entry against LAG Interface. |
| Workaround | Disable IP Source-guard on the VLAN before removing the physical port from LAG. Enable IP Source-guard on the VLAN later. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-178487 |
|---|---|
| Symptom | Unable to modify LAG membership for ports which are part of a VLAN and IP Source-guard is enabled on the VLAN. Below error message is thrown while trying to add a additional port to LAG interface.<br>"Source Guard is configured on secondary port 12/1/47" |
| Condition | IP Source-guard is enabled on a VLAN and LAG interface is part of the VLAN.<br>Adding another port to the LAG interface will result in above error condition |
| Workaround | Remove IP Source-guard on the VLAN before adding new ports to the LAG interface |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-178347 |
|---|---|
| Symptom | When community string more than 32 characters is configured, the device unexpectedly reloads |
| Condition | Configure "snmp-server host x.x.x.x version v2c [community]" cli command with community string more than 32 characters |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.40 |
| Technology/ Technology Group | Management - SNMP - Simple Network Management Protocol |

| Issue | FI-178385 |
|---|---|
| Symptom | Logging on one or more ACLs will not work when the logging is enabled on a LAG interface. |
| Condition | It happens on a switch image. It happens on a LAG interface. It happens when there are multiple per-VLAN configurations of ACLs existing. It happens when the logging is finally enabled, |
| Workaround | Enabling logging on the interface prior to configuring the ACLs will avoid running into this issue. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-178355 |
|---|---|
| Symptom | After upgrading ICX from FI8050 to FI8070, ICX does not obtain Dynamic IP Address after removing all static IP addresses assigned and disabling DHCP server |
| Condition | This issue is seen when device has FI8050 image with DHCP server and static IP configured in the device before upgrading to FI8070. Issue is not seen if DHCP server is not enabled in the device before upgrading. |
| Workaround | |
| Recovery | Disable DHCP client and re-enable to resolve the issue. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-178319 |
|---|---|
| Symptom | Unintended multicast traffic flooding and forwarding on a port transitioning from a stack port configuration to a data port. |
| Condition | 1) A stack with a ring or linear configuration<br>2) Convert a already configured stack port to a data port on the active.<br>3) Layer 2 multicast configuration present in the system |
| Workaround | |
| Recovery | Remove the multicast configuration and reapply configuration on the desired interfaces. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-178279 |
|---|---|
| Symptom | ACL Accounting Counters are continuously incrementing on Port Extender (PE) port even after the traffic stops hitting the ACL. |
| Condition | IPv4 ACL or IPv6 ACL with Accounting enabled is applied on Port Extender (PE) port. It is applied either directly on the PE physical port or on a Virtual VE port of which the PE port is member.<br>Traffic is Ingressing on the PE port and ACL Accounting Counters are incremented as expected.<br>Once the traffic stops Ingressing on the PE port, ACL Accoutning Counters are still incrementing |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |

| Issue | FI-177775 |
|---|---|
| Symptom | When user configures global DSCP remarking and multiple ports of a stack unit belong to a vlan then traffic from not all ports in that unit is getting remarked as expected. Traffic from lowest port in a stack unit that belong to the vlan will be DSCP remarked and the traffic from the rest of the ports will not be DSCP remarked to the configured value. |
| Condition | For user to encounter this issue following conditions should be met<br><br>1. Multiple ports from a stack unit should belong to a vlan<br>2. Global DSCP should be configured<br>3. There should not be any IPv4 ACL associated with virtual router interface for this vlan |
| Workaround | User can configure global DSCP remarking first and then configure Vlan and add members to avoid running into this issue. |
| Recovery | The user can reload the stack units to which members of the vlan belong to, to recover from this issue. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-177537 |
|---|---|
| Symptom | Tunnel source interface with primary lag interface is lost during software release upgrade. |
| Condition | When ICX device is upgraded from any release prior to 8.0.61 with tunnel source interface as primary lag interface, the configuration is lost. |
| Workaround | None |
| Recovery | Reconfigure the tunnel source interface with the correct lag interface after the upgrade. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-177089 |
|---|---|
| Symptom | Power pre allocation for a 4pair port that is converted to 2pair port using "interface-mode-2pair-pse" is 95W |
| Condition | Though 4pair port is converted to 2pair port, the power pre allocation is 95W. |
| Workaround | use "inline power power-limit 30000" to avoid pre-allocation of 95W and also power reservation of 95W for 2pair class 4 PD. |
| Recovery | use "inline power power-limit 30000" to reduce the power reservation for 2pair class 4 PD. |
| Probability | |
| Found In | FI 08.0.70 |

| Issue | FI-112367 |
|---|---|
| Symptom | System resets while running PIM protocol. |
| Condition | The system rarely resets when multiple multicast receivers keep moving from L3 receivers (source in different vlan) to L2 receivers (source in same vlan) and vice versa. This is applicable to all ICX7xxx products running router image. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Stacking - Traditional Stacking |

| Issue | FI-176976 |
|---|---|
| Symptom | IPv6 Hosts within a sub-net on a broadcast network is not reachable via non-DR router in a LAN. |
| Condition | IPv6 Sub-net address is not configured on the all the connected router's interface in LAN. This problem is applicable on all products on router image using IPv6 starting 8.0.30, 8.0,40, 8.0.50, 8.0.60 and 8.0.61. |
| Workaround | Configure the affected sub-net IP address on all the connected router's interface in LAN. |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-176214 |
|---|---|
| Symptom | Unexpected reload of the ICX device would be experienced when MAC-Authentication fails |
| Condition | PC is behind IP Phone and Flex-Authentication Order is Mac-Authentication followed by Dot1x. Non-Dot1x Capable IP Phone has Mac-Authentication sessions for both Data and Voice-Vlan. Mac-Authentication for PC is Failed and Dot1x Authentication is Succeeded with Dynamic Vlan. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.40 |
| Technology/ Technology Group | Security - 802.1x Port-based Authentication |

| Issue | FI-176658 |
|-------|-----------|
| Symptom | IP-MAC is not used for L3 Unicast Data and Control packets. |
| Condition | L3 Unicast Data and Control packets may fails to use the ip-mac configured on the l3-interface configured on a LAG after reload of the system. This is applicable to all ICX7xxx products running router image on 8061x release. |
| Workaround | None |
| Recovery | Re-configure IP-MAC on the interface. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | IP Multicast - IPv4 Multicast Routing |

| Issue | FI-176617 |
|-------|-----------|
| Symptom | ICX device does not obtain dynamic IP Address automatically, when a static IP address is un-configured in the device |
| Condition | Observed when the static IP address is un-configured after enabling the dhcp client in the device. |
| Workaround | |
| Recovery | Disable the DHCP client globally and re-enable the DHCP Client |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Layer 3 Routing/Network Layer - DHCP - Dynamic Host Configuration Protocol |

| Issue | FI-176492 |
|-------|-----------|
| Symptom | System Reset with PIM running. |
| Condition | System resets while executing "clear ip/ipv6 pim mcache" with IP Multicast traffic running (having active mcache and pim groups table). This due to some time latency so can happen occasionally, on all ICX7xxxx products running router image and  applicable to all releases post 8030. |
| Workaround | Avoid executing "clear ip/ipv6 pim mcache" |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-176375 |
|---|---|
| Symptom | System Resets when OSPFv3 IPSEC authentication configuration is removed from an interface viz. no ipv6 ospf authentication ipsec ... |
| Condition | If IPSEC authentication is disabled and key change timer is configured as 0 and then IPSEC configuration is removed from an OSPFv3 enabled interface viz. no ipv6 ospf authentication ipsec .. system will reset. This problem is applicable to all ICX products running router image starting 8.0.0 release. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-176371 |
|---|---|
| Symptom | Active unit crashes sometimes during reload due to a timing condition when the IPSG feature is enabled with large ACL on a VE. |
| Condition | 1. IPSG and ACLs should be bound on a VE. The probability of hitting this issue is higher if the no.of such VE's is more. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-176369 |
|---|---|
| Symptom | Member unit reloads upon configuring a scaled ACL consisting of more than 250 filters on default VLAN containing almost all ports of the system. |
| Condition | Configuring a scaled ACL consisting of more than 250 filters on default VLAN containing almost all ports of the system. |
| Workaround | Create the ACL with fewer filters and apply it to the default VLAN. Thereafter, add additional filters to the ACL individually. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-176364 |
|---|---|
| Symptom | The ACL remains operational in hardware even after the ACL is implicitly removed from the running configuration. |
| Condition | The ACL is configured on the LAG interface and then all ports in the LAG are removed, one by one. This does not happen always. It only happens under certain timing conditions |
| Workaround | Unconfiguring the ACL from the LAG interface first before removing all ports from the LAG will avoid running into this issue. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-176342 |
|---|---|
| Symptom | Unexpected reload of SPX active cb when an unsupported feature trace-l2 is received on a SPX system. |
| Condition | 1) Reception of trace-l2 packet from the peer 2) l2-trace processing of the received packet 3) Response to the trace-l2 packet on a PE port results in the unexpected reload. |
| Workaround | Unconfigure trace-l2 feature if already configured. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-175500 |
|---|---|
| Symptom | On reload, additional DSCP remarking rules are configured in the TCAM. These additional entries are not getting removed even when DSCP remarking is un-configured. This results in traffic getting DSCP remarked even after un-configuring DSCP remarking feature after removing the ACL bound to the Router Interface of the vlan. |
| Condition | User will encounter this issue only when below steps are followed<br>1. Configure DSCP remarking at global level<br>2. IPv4 ACL must be configured on the router interface of a vlan<br>3. Reload the system<br>4. Remove DSCP remarking at global level after reload<br><br>The traffic will still be getting DSCP remarked after the IPv4 ACL is removed. |
| Workaround | To avoid running into this issue, before issuing a reload, un-configure global DSCP remarking and re-configure DSCP remarking after reload. |
| Recovery | User should reload stack units to which the members of the vlan belong to, to recover from this issue. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-175082 |
|---|---|
| Symptom | In ICX7450 and ICX7250 pass-thru L2 GRE packet are getting dropped. |
| Condition | L2 GRE traffic over ICX7450 and ICX7250. This is applicable to start 8.0.20/ICX7450 and 8.0.30/ICX7250 release on a router image. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-174980 |
|---|---|
| Symptom | System reset sometime when Vlan is deleted that is being used by Multicast. |
| Condition | User deleting a Vlan being used by Multicast. |
| Workaround | N.A. |
| Recovery | N.A. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-174970 |
|---|---|
| Symptom | On moving a port from Default VRF to User-configured VRF, TCP Syn and ICMP Smurf attack prevention configured on the port are not removed (Unlike many other configurations) |
| Condition | 1. A Port is part of Default VRF. 2. ICMP Smurf attack or TCP Sync Attack Prevention is configured on the port 3. Port is added to User configured VRF and the above settings are still there. |
| Workaround | Remove ICMP and TCP Syn attack Prevention on the port before moving the port to User configured VRF |
| Recovery | Remove ICMP and TCP Syn attack Prevention on the port after moving the port to User configured VRF |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-168927 |
|---|---|
| Symptom | A stack unit on an ICX stack crashes under certain timing conditions when deleting a filter from a large ACL that was bound to an interface. |
| Condition | 1. ACL should have at least 100 filters or more. 2. A filter is inserted at the beginning of the ACL and should result in the priority update for the rest of the filters below it. 3. A filter should have been deleted from middle for which the priority update is about to happen. |
| Workaround | None |
| Recovery | The unit recovers itself and becomes operational again. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-168914 |
|---|---|
| Symptom | In a switch with DHCP snooping configured, if a DHCP client sends a DHCP Request packet, and the server sends a DHCP ACK packet containing several DHCP options with Option 51 exceeding the byte offset of 64 in the DHCP options, the switch will not be able to process option 51 lease duration. |
| Condition | In a switch with DHCP snooping configured, if the DHCP ACK packet from the server contains multiple DHCP options such that option 51 exceeds an offset of 64 among the DHCP options, the option 51 containing Lease Duration is not processed correctly |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-122466 |
|---|---|
| Symptom | In a switch port extender (SPX) setup with ICX7250 as a port extender (PE) when the SPX formation happens then the ICX7250 goes for sudden reload with error message |
| Condition | This problem happens sometimes when we try to bring up the switch port extender (SPX) setup with ICX7250 as a port extender (PE) |
| Workaround | |
| Recovery | None |
| Probability | Medium |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-168567 |
|---|---|
| Symptom | On member unit, ACL changes are not reflected in the Hardware TCAM |
| Condition | Apply ACL on member unit port and Perform regenerate sequence number operation on the applied ACL. Try to delete a filter in that ACL using new filter id. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-157788 |
|---|---|
| Symptom | In a switch image, when PCP remarking is configured on a port with egress ACL already bound, the traffic will not get remarked as configured. |
| Condition | User will encounter this issue if an egress ACL is configured on the port first and then later PCP remarking is configured on the same port. |
| Workaround | User can configure PCP remark first and then bind egress ACL to the port |
| Recovery | User can un-bind and rebind the egress ACL on the port to recover from this issue. |
| Probability | Medium |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-157677 |
|---|---|
| Symptom | Forwarding based on LAG under in ICX 7150 between ports of 1G and 2.5G does not work after reload. |
| Condition | 1) ICX7150 with auto speed configured on ports<br>2) Lag configuration exists between 2 ports of 1G and 2.5G speed<br>3) Reload the box<br>4) Lag formation between the 2 ports mentioned in step 2) fails. |
| Workaround | Force the speed of individual ports on the LAG to the desired speed. Do not use auto speed. |
| Recovery | The ports under consideration need to be added back to the lag. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-114075 |
|---|---|
| Symptom | The Digital Optical Monitor commands like "optical-monitor enable" is not supported for stacking ports on ICX7xxx series platforms |
| Condition | The Digital optical monitoring commands like "optical-monitor enable" is not supported on any stacking ports |
| Workaround | In order to run the optical-monitoring commands on a stacking port, user need to unconfigure stacking on that port and then run this command |
| Recovery | None |
| Probability | Low |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-118029 |
|---|---|
| Symptom | When openflow L2 mode is enabled on a member unit port, ping to that port's IP address succeeds. Also ARP table is populated for the same. This causes the non openflow ports be able to send unicast traffic to the IP learnt (in ARP table) on openflow port. |
| Condition | 1) Openflow is enabled on the member unit port. 2) IP address is configured on openflow interface. 3) ARP should be resolved before sending the traffic. |
| Workaround | By configuring openflow in L23 mode on that port, this issue can be avoided. |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-120893 |
|---|---|
| Symptom | When a dead Radius Server comes back up and tries to apply ACL as part of authentication for a user that was already authenticated with Auth timeout success, the ACL does not get applied. |
| Condition | When Auth timeout action is SUCCESS and a dead Radius server comes back up and attempts to apply ACL for the authenticated user. |
| Workaround | Reload the stack units |
| Recovery | None |
| Probability | Low |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-120447 |
|---|---|
| Symptom | A new filter added to an ACL which pertains to an IPSG entry which is earlier in the sequence order of IPSG entries bound does not get applied |
| Condition | IPv4 Filter is added to an existing configured ACL after IPSG binding happens |
| Workaround | Remove and reapply the ACL |
| Recovery | None |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-121471 |
|---|---|
| Symptom | While authenticating the username and password using Radius over TLS secure connection, authentication fails with error message "ERROR: TLS Alert read:fatal:bad certificate" |
| Condition | Configure ICX device with command "radius-server host <IP address> ssl-auth-port <port numebr> authentication-only" and "aaa authentication login default radius" to authenticate Username and password via encrypted radius, Which fails always while establishing TLS connection. |
| Workaround | |
| Recovery | |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-117970 |
|---|---|
| Symptom | The 40Gbps 10 Meter Active Optical Cable (AOC) does not work reliably on ICX7450 40G port configured as a stacking port. When 10 meter AOC cable is used on ICX7450 40G stacking port then sometime the port flap (port going up and down continuously) is observed |
| Condition | This issue happens on ICX7450 40G port connected with 10 meter Active optical cable and the port configured as a stacking port |
| Workaround | The 10 meter AOC cable does not work on ICX7450 40G stacking port. The 1 meter, 3 meter, 5 meter AOC cables works fine so the user can use these AOC cables. Otherwise the user can use other supported SR4 or LR4 optics there |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-119149 |
|---|---|
| Symptom | Error message indicating acl hardware resource error is seen and some filters do not get programmed |
| Condition | When traffic policy ACL is already applied on the interface and ACL with accounting enabled is applied on interface. |
| Workaround | None |
| Recovery | Remove traffic policies. Remove and add filters which are not programmed properly. |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-123182 |
|---|---|
| Symptom | CPU sample is turnoff by default |
| Condition | CPU sampling is turnoff by default |
| Workaround | If CPU sampling is needed, need to turn it on manually. |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-120235 |
|---|---|
| Symptom | PoE Overdrive request from Ruckus R720 is not honored by ICX-7450 32ZP |
| Condition | The power request from R720 is not matching the requirement. Also this feature is not supported on the ICX 7450-32ZP in 8061. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-115211 |
|---|---|
| Symptom | In a switch port extender setup where ICX7450 is configured as a port extender, when 4x10G fiber module is connected to ICX7450 and the LRM adapter is connected in that module then this connection is not supported. But in the "show media" command line output the error information about unsupported adapter is not shown. |
| Condition | This issue happens when ICX7450 is configured as a port extender in a switch port extender setup and that switch has 4x10G fiber module connected with LRM adapter plugged in there. |
| Workaround | User can take out the ICX7450 unit from SPX setup and then run the same command line "show media" to see if the connected LRM adapter on ICX7450 4x10F module is valid or not |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-118411 |
|---|---|
| Symptom | Filter rules are not cleared from Hardware TCAM when the User's session is destroyed |
| Condition | Flexauth Port, having sessions, is disabled |
| Workaround | Reload the stack units |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.50 |
| Technology/ Technology Group | |

| Issue | FI-121719 |
|---|---|
| Symptom | On the ICX7150 if LRM adapter is connected to it without the fiber cable connection on the LRM adapter's line side then on the ICX7150 side the port LED remains Up |
| Condition | This issue happens on the ICX7150 when the LRM adapter is connected to ICX7150 without fiber cable connected to LRM adapter |
| Workaround | None |
| Recovery | None |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-121571 |
|---|---|
| Symptom | Member unit reloads upon configuring a scaled ACL consisting of more than 250 filters on default VLAN containing almost all ports of the system. |
| Condition | Configuring a scaled ACL consisting of more than 250 filters on default VLAN containing almost all ports of the system. |
| Workaround | Create the ACL with fewer filters and apply it to the default VLAN. Thereafter, add additional filters to the ACL individually. |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-116795 |
|---|---|
| Symptom | Error traces might be observed randomly - "Error: remaining ticks (0) is smaller than elapsed ticks" |
| Condition | Switch is up and running for 621 days or more. |
| Workaround | Reboot before 621 days of system up time. If reboot was not done in 621 days and after that if errors are seen, then also reboot system. |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | |

| Issue | FI-122099 |
|---|---|
| Symptom | High CPU for 2 to 3 minutes and inter-VLAN traffic leak, with OpenFlow configured on an Campus Fabric(SPX) system. |
| Condition | Configuring OpenFlow on Campus Fabric with traffic can expose this problem. |
| Workaround | |
| Recovery | From FastIron release 8.0.70 onward, configuring Campus Fabric and OpenFlow features together is not supported. |
| Probability | Medium |
| Found In | FI 08.0.50 |
| Technology/ Technology Group | |

| Issue | FI-114579 |
|---|---|
| Symptom | In the ICX7750 stack when the whole stack is upgraded with the new u-boot image and reloaded. After the system comes up then if the user tries to boot up standby unit from a particular partition by issuing a command from Active unit then the standby unit gets booted with older u-boot image |
| Condition | This issue is seen in ICX7750 stack when the whole stack is upgraded with new u-boot image and then if the user tries to boot up standby unit from a particular partition by issuing command from Active unit |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.60 |
| Technology/ Technology Group | |

| Issue | FI-115617 |
|---|---|
| Symptom | Upgrading Flash Image with TFTP-TELNET from BNA is not Working |
| Condition | 1. Discover device in BNA. 2. Select transfer options as Telnet-TFTP 3. Select 'save and reload' option. 4. Load flash image from BNA to primary of device. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | |

| Issue | FI-121740 |
|---|---|
| Symptom | On ICX7150-48ZP unit 2.5G port when the continuous traffic is run for long duration then sometimes the CRC error is observed on these 2.5G port |
| Condition | This issue happens on ICX7150-48ZP 2.5G port when continuous traffic is run for long time |
| Workaround | |
| Recovery | |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-123994 |
|---|---|
| Symptom | While doing ISSU, it gets aborted and IPv4/IPv6 traffic stop forwarding for the unit under upgrade. |
| Condition | ISSU operation on router image on 8050, 8060 or 8061 on all ICX7xxx products with routing enabled due to certain time latency of event processing in the system we can rarely see ISSU aborting with IPv4/IPv6 traffic disruption. |
| Workaround | None |
| Recovery | Reload the whole stacking system. |
| Probability | High |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-122450 |
|---|---|
| Symptom | spx interactive-setup will not be able to discover the PEs attached on this spx-port, if spx-port is removed and then added again as spx-port, |
| Condition | While using spx interactive-setup if user changed spx-port to data-port and then spx-port, spx interactive-setup will not be able to discover the PEs attached to this spx-port |
| Workaround | |
| Recovery | Related PE unit can be reloaded to correct the issue. |
| Probability | Medium |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-121851 |
|---|---|
| Symptom | Authenticated user session does not move from an existing port to a new one. |
| Condition | Attempt to move an authenticated user to a new port. |
| Workaround | Clear the User session on the old port before movement |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-122251 |
|---|---|
| Symptom | A phone connected to a Flexauth port is unable to access the network and LLDP packets are dropped from this device |
| Condition | Phone is trying to authenticate on a Flexauth port |
| Workaround | configure lldp-passthrough on the Flexauth port |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-122138 |
|---|---|
| Symptom | Authenticated user with radius returned ACL observes traffic issues, where traffic handling is not as per the configured ACL. |
| Condition | Dot1x / macauth users needs to be get authenticated with radius returned ACLs.<br><br>A second user is getting authenticated at the same time as first user. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-122083 |
|---|---|
| Symptom | The ICX SNMP agent with STP configured on LAG interface, does not list the lag ports in response for SNMPWALK request on dot1dStp MIB table. |
| Condition | Observed when STP is configured on the lag interface in ICX device. |
| Workaround | |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-122836 |
|---|---|
| Symptom | Memory leak is observed |
| Condition | when 25 dot1x sessions churn over 16hrs of longevity run |
| Workaround | Reload the stack units |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.40 |

| Issue | FI-122753 |
|---|---|
| Symptom | In a switch port extender setup where ICX7450 or ICX7250 is configured as port extender, when the EEE (Energy efficient ethernet) command is applied globally on the whole SPX setup then in one corner case where one of the port extender reloads due to some memory issue, that unit can not join back the SPX stack as the unit keeps attaching and detaching the SPX stack continuously. |
| Condition | This is a corner case which happens in Switch port extender setup having ICX7450 or ICX7250 have a global configuration for EEE enabled and then due to some memory issue one of the port extender ICX7450/ICX7250 unit reloads. |
| Workaround | The user can remove the global EEE configuration to avoid this problem |
| Recovery | |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-122803 |
|---|---|
| Symptom | ICX DHCP client running switch image is not reachable, since IP is lost after moving to different network |
| Condition | Moving ICX DHCP client to a different network after obtaining dynamic IP address from one network. |
| Workaround | |
| Recovery | Disable and enable the DHCP client |
| Probability | Medium |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-108037 |
|---|---|
| Symptom | The link does not come up between ICX7450-32ZP 2.5G port and ICX7750-48C 10G copper port connected using Crossover Ethernet cable with ports configured in 1G speed using "speed-duplex 1000-full-master" command |
| Condition | This issue happen in a connection between ICX7450-32ZP and ICX7750-48C using Crossover Ethernet cable and ports configured in 1G mode |
| Workaround | Use straight RJ45 cable or use the full crossover RJ45 cable for connecting the ICX7450-32ZP 2.5G port |
| Recovery | |
| Probability | Medium |
| Found In | FI 08.0.40 |
| Technology/ Technology Group | |

| Issue | FI-112027 |
|---|---|
| Symptom | Applying filter for CLI output using pipe ( | ) doesn't work on Telnet session for flex authentication commands |
| Condition | Executing Flex authentication command in telnet session and apply output filtered using pipe (|) will not work |
| Workaround | Execute the Flex authentication commands in console session if output has to be filtered using pipe (|). |
| Recovery | |
| Probability | High |
| Found In | FI 08.0.60 |
| Technology/ Technology Group | |

| Issue | FI-115744 |
|---|---|
| Symptom | When a new source starts sending IP Multicast traffic, registration process may take few seconds and it can lead to software forwarding of traffic for that duration. |
| Condition | When a new source starts sending IP Multicast traffic, RP system may take few seconds to send join message to FHR as part registration process. Till registration process is ongoing, the traffic will be software forwarded. This problem is applicable for all products and all releases before 8070. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.50 |
| Technology/ Technology Group | |

## Known issues in release 08.0.70

This section lists open software defects with Critical, High, and Medium Technical Severity as of December 21, 2017 in 08.0.70.

| Issue | FI-181697 |
|---|---|
| Symptom | System reloads or switchover to new active. |
| Condition | When underlying topology is not stable OSPFv3 LSAs may loop causing lot of LSAs pending for transmission per interface. In this condition system may reload or switchover to new active. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181611 |
|---|---|
| Symptom | 'Session-Timeout' attribute is not updating the re-authentication period for the 802.1x authenticated User |
| Condition | When 'Session-Timeout' attribute is sent by Radius-Server for an 802.1x authenticated User |
| Workaround | Set the 'Session-Timeout' value to re-auth period from CLI |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181603 |
|---|---|
| Symptom | On ICX7650 1G copper port. When the port is configured at 100 Mbps full duplex mode and connected to link partner which is also configured at 100 Mbps full duplex mode with auto negotiation disabled. Then if the EEE (energy efficient ethernet) is enabled globally, the port goes to 100 Mbps half duplex mode. |
| Condition | The problem happens only when auto negotiation is disabled on the link partner and EEE configuration is enabled globally on the ICX 7650 1G port along with fixed 100 Mbps full duplex mode configuration. |
| Workaround | None |
| Recovery | If a port gets into the mentioned symptom, follow the below steps for recovery. 1) "disable" the port. 2) Run the command "no eee" on the port. 3) "enable" the port. |
| Probability | |
| Found In | FI 08.0.70 |

| 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.<br><br>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 08.0.70 |
| Technology/ Technology Group | Other - Other |

| Issue | FI-181565 |
|---|---|
| Symptom | On ICX7650, if the stacking trunk is configured, and trying to do unit replacement on standby unit, could causes the protocols packet not reaching the standby unit. |
| Condition | This issue is observed only when stacking trunk is configured and unit replacement is done for the standby unit. |
| Workaround | None |
| Recovery | Reload the standby unit will recover from this condition |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | IP Multicast - IGMP - Internet Group Management Protocol |

| Issue | FI-181555 |
|---|---|
| Symptom | When source guard is enabled on the ve interface, some features, for example PBR. |
| Condition | source guard is enabled on VE.<br>PBR is applied on lag interface or physical interface. |
| Workaround | 1) Remove the source guard enable on ve, add PBR and apply back the source guard. |
| Recovery | 1) Remove the source guard enable on ve, add PBR and apply back source guard.<br>2) Add and remove any feature f.e. an ACL or PBR on an Ve interface and remove it. This will nullify the error condition. |
| Probability | |
| Found In | FI 08.0.80 |

| Issue | FI-181531 |
|---|---|
| Symptom | The output of "show ip tcp connections" shows "RxBuffer" value as a negative number. This is a printing error and there is no functional impact.<br>For example,<br>telnet@Router#show ip tcp connections<br>Total 8 TCP connections<br>    LISTEN: 5; SYN-SENT: 0; SYN-RECEIVED 0; ESTABLISHED: 3; FIN-WAIT-1: 0<br>    FIN-WAIT-2: 0; CLOSE-WAIT: 0; LAST-ACK 0; CLOSING: 0; TIME-WAIT: 0<br>Local IP address:port <-> Remote IP address:port TCP state    RcvQue RxBuffe SendQue TxBuffe<br>10.20.78.149    443    10.20.74.8   37712  ESTABLISHED  0     -2   0     0<br>0.0.0.0          443    0.0.0.0      0    LISTEN    0   -2   0   0 |
| Condition | This printing error may be seen in the output of "show ip tcp connections" after multiple TCP connections have been established and torn down. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181526 |
|---|---|
| Symptom | MACSec FIPs KAT test takes few minutes (to the order of 5 minutes) to complete in FIPs mode |
| Condition | Boot ICX 7650 in FIPs mode with LRM optic on the 10G ports |
| Workaround | Remove LRM optic during bootup and insert back after KAT test is complete |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - FIPS - Federal Information Processing Standards |

| Issue | FI-181520 |
|---|---|
| Symptom | MACSec KAT test does not run on non-active units of an ICX 7650 stack. However MACSec is supported on all units in the stack |
| Condition | Booting up ICX 7650 stack in FIPs mode |
| Workaround | Run FIPs tests in standalone mode to validate the device. |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - FIPS - Federal Information Processing Standards |

| Issue | FI-181508 |
|---|---|
| Symptom | When multiple telnet sessions are opened and multiple configuration download operations are done, system can go into a state where it continuously prints "Failed to open gpio value for reading". |
| Condition | When multiple telnet sessions are opened and multiple configuration download operations are done, system can continuously print "Failed to open gpio value for reading". |
| Workaround | Do not run multiple configuration downloads from multiple telnet sessions simultaneously . |
| Recovery | Reload the system to recover from this state. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181506 |
|---|---|
| Symptom | |
| Condition | This can be seen on a stack with FIPS or CC mode enabled, during reload. This can also be seen when executing the "fips zeroize" command on a stack. |
| Workaround | |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - FIPS - Federal Information Processing Standards |

| Issue | FI-181502 |
|---|---|
| Symptom | When ICX7150 is continuously reloaded in a loop using scripts, occasionally software watchdog expiry is observed which lead to the system reset and sometime kernel exceptions. |
| Condition | The probability to see this issue in 8.0.70 release is very remote since workaround solution is already implemented in this release. |
| Workaround | None |
| Recovery | System will automatically recover after the reboot |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181466 |
|---|---|
| Symptom | Following error messages displayed on Console/telnet/ssh: 0:_soc_mem_write_sanity_check: soc_mem_write: invalid index 87617 for memory L2_ENTRY_ONLY_ECC 0:_soc_ser_sram_correction: SER SRAM correction encoutered error(-4) in mem write |
| Condition | There are no specific user triggers as this is a hardware single bit error and can happen due to changes in atmosphere. |
| Workaround | |
| Recovery | Single Bit Error recovery in software automatically recovers the single bit error and error message stop after some time. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Monitoring - OAM - Operations, Admin & Maintenance |

| Issue | FI-181383 |
|---|---|
| Symptom | The message "all 2 display buffers are busy, please try later" is observed in a telnet session. |
| Condition | When running 12 concurrent telnet sessions with each executing commands with large volume of output (such as "supportsave" and "show tech") the issue was seen after an hour. |
| Workaround | When running commands with potentially large volume of output ( such as "supportsave", "show log" and "show tech"), ensure that they are not running concurrently on more than 1 telnet session. |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181332 |
|---|---|
| Symptom | On ICX7450 platform when the external USB is plugged in and the FIPS mode is enabled then some time the message is seen on console indicating the external USB has been plugged out "External USB-Mass-Storage Plugged-out" |
| Condition | This issue happens rarely on ICX7450 platform when the external USB storage device is plugged in and the FIPS mode is enabled |
| Workaround | The message does not have any functional impact, there is no workaround |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181273 |
|---|---|
| Symptom | CLI Filters like "inc/exc" doesn't work for macsec statistics for non-active unit ports |
| Condition | Give "show macsec stat" command on non-active units with CLI Filters like inc/exc |
| Workaround | Use filter option if needed from active console. |
| Recovery | No functional impact. show commands are typically done on active console. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - MACsec - Media Access Control security |

| Issue | FI-181260 |
|---|---|
| Symptom | New standby CPU of about 47% is observed after switch over. with BGPv6 configured over IPSec V6 tunnel. No other functional impact seen. |
| Condition | 1) A device with a IPSec V6 tunnel with BGPv6 configured on the tunnel.<br>2) Perform a stack switch over. |
| Workaround | None |
| Recovery | Clear all the IKE session with BGP configured on it in the new active shall recover from high CPU on the standby. |
| Probability | |
| Found In | FI 08.0.70 |

| Issue | FI-181256 |
|---|---|
| Symptom | IPv6 traffic with packet size lesser than 84 bytes are not being logged when ACL logging is enabled |
| Condition | 1. Configure IPv6 ACL with logging enabled.<br>2. Bind the ACL to interface.<br>3. IPv6 traffic matching the IPv6 ACL will be trapped to control CPU for processing but logging fails due to validity checks failing for packets lesser than 84 bytes. |
| Workaround | None |
| Recovery | None.<br>No functional impact. ACL logging will not show logs for these packets. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181250 |
|---|---|
| Symptom | When only boot code on flash is different from manifest-location and ICX system images are same, then also manifest downloads both boot code & ICX images |
| Condition | Upgrade the ICX software using the manifest file update option |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Other - Other |

| Issue | FI-181214 |
|---|---|
| Symptom | When there is a loop in management port network or there is a very high traffic in management port, the ICX7250 unit can crash |
| Condition | When there is a loop in management port network or there is a very high traffic in management port, the ICX7250 unit can crash |
| Workaround | Avoid loop in the network where management port is connected. |
| Recovery | After the crash, the unit automatically recovers. Refer workaround to avoid this again. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181199 |
|---|---|
| Symptom | PBR configured on a LAG interface of a reloaded unit are not programmed correctly. |
| Condition | PBRv4 or PBRv6 is applied on lag interface. Lag has ports on the unit that is going for reload. Next hop outgoing interface is not on the reloaded unit. Reload the unit |
| Workaround | Remove PBR configuration from LAG before reload and then re-configure PBR after reload for the LAG interface. no ip policy route-map <route-map-name> or no ipv6 policy route-map <route-map-name> |
| Recovery | After reload of unit, if PBR is not programmed on the interface, remove and re-apply the PBR policy on interface. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181159 |
|---|---|
| Symptom | After stack switchover, next hop entries corresponding to tunnels remain in hardware and cpu utilization is at 9 or 10%. |
| Condition | 1. With IPSec Tunnel configured and PBR using IPSec tunnel as next hop, if switchover is performed, next hop entry is not getting deleted. 2. sh cpu shows high utilization at 9-10%. This is seen with first switch over. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181137 |
|---|---|
| Symptom | Key used by OSPF and provisioned in key chain will be different.after Switcher/Fail over/ISSU as applications like OSPFv2/OSPFv3 that uses key-chain does not find a valid key to use for packet authentication, this may also result in adjacency flap. |
| Condition | When key-ids inside the key-chain are configured with expire time less than 10 seconds for all the keys and performing switch over or Fail over or ISSU. |
| Workaround | Key-ids inside a key-chain needs to be configured with expire time greater than 10 sec. |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |

| Issue | FI-181070 |
|---|---|
| Symptom | L2QVLAN sub-option for option 176 will be missing in the DHCP ACK packet. |
| Condition | When FastIron device is used as DHCP server with option 176 configured, L2QVLAN field will be missing in the DHCP ACK packet. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-181060 |
|---|---|
| Symptom | -Issue a boot image download.<br>-While the boot image sync is going on, issue another boot image download.<br>-At this point we will get the error !!!INFO: Flash access in progress, please wait...<br>-Keep trying to download the image continuously inspite of the warning, at some point you will hit the crash. |
| Condition | The router crash. |
| Workaround | Avoid repeated boot download request if the previous boot has not finished. |
| Recovery | Reload |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Stacking - Mixed Stacking |

| Issue | FI-181047 |
|---|---|
| Symptom | LAG ports go into blocking state with MACSec configured on a LAG between ICX 7450 and ICX 7650 |
| Condition | 1. Have traffic on the LAG between the devices<br>2. Reload or perform ISSU of the ICX 7650 |
| Workaround | Stop traffic on the Inter switch link-LAG in this case before a reload or performing ISSU |
| Recovery | Flap the LAG interface using a disable/enable |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Layer 2 Switching - LAG - Link Aggregation Group |

| Issue | FI-180995 |
|---|---|
| Symptom | DHCP Server options 16, 28 and 32 are allowed to be configured with more than one IP address. |
| Condition | When FastIron device is used as DHCP Server, the options 16, 28 and 32 can be configured with more than one IP address. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180921 |
|---|---|
| Symptom | An error is displayed when applying an IPv6 ACL on the VE interface when there is already an existing IPv6 ACL on same interface. The error message is similar to the following message:<br><br>ICX7450-24 Router(config-vif-499)#ipv6 traffic-filter scale1 in Insufficient hardware resources to apply the V6 ACL. Please remove already applied ACL(s) and/or Security features and try again. ERROR: Insufficient hardware (TCAM) resource on unit 60028 for binding the IPv6 ACL scale1 to interface 499.<br><br>SYSLOG: <10> Nov 11 04:59:23 ERROR: Insufficient hardware (TCAM) resource on unit 60028 for binding the IPv6 ACL scale1 to interface 499.<br><br>On the data path, the new ACL will not be programmed into TCAM and the old ACL rules still persist. |
| Condition | 1. Configure and apply an IPv6 ACL on VE interface<br>2. Now apply another IPv6 ACL on VE interface which has logging enabled. |
| Workaround | Do not enable logging on the IPv6 ACL |
| Recovery | 1. Remove the already existing IPv6 ACL applied on VE interface.<br>2. Apply the new IPv6 ACL on VE interface.<br><br>The Hardware TCAM entries should reflect the new IPv6 ACL FP entries. The traffic flow will match the new IPv6 ACL entries in TCAM. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180240 |
|---|---|
| Symptom | "show ip ssl" command displays two SSL/TLS session established for the same TLS server. Sample output during issue: show ip ssl Session  Protocol Source IP          Source Port  Remote IP Remote Port 1     TLS_1_2  10.21.240.11          645       10.21.240.39 5002 2     TLS_1_2  10.21.240.11          643       10.21.240.39 5002 There is no impact on the traffic between the TLS client and TLS server |
| Condition | Issue is observed when Step 1. SSL Session is already established, and Step 2. The server certificate is modifed, and Step 3. The SSL session is re-established If "show ip ssl" is run after the above steps, the old session will be seen along with the new session. |
| Workaround | None |
| Recovery | Issue will auto-resolve when the session rekey happens after one hour. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180871 |
|---|---|
| Symptom | Duplicate packets will be received for a short window of  7 milliseconds at the device connected to this switch. Applications using Ping or any UDP based applications will report error on duplicate packet reception. |
| Condition | Flap a link which connected to an active unit of a peer switch of a VRRP router. And MSTP admin-pt2pt configured on all the relevant ports of both the systems. Problem is seen when the link comes back up up, and there could  be a momentary duplication of L2 frames for around 7 milliseconds. |
| Workaround | If possible, do not configure ports on the system as MSTP admin-pt2pt-mac ports. |
| Recovery | This packet duplication happens for a very short time window of 7 milliseconds and system recovers there after. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180767 |
|---|---|
| Symptom | 1. Error message on member console indicating ACL programming failed to<br>  program on an interface, such as<br>   "Unable to update the TCAM with the ACL filters"<br><br>2. Traffic treatment not inline with the applied ACLs on some member ports in the stack after a stack reload.<br><br>3. Failure to program the ACL applied on default VLAN immediately upon reload. |
| Condition | 1. On stack reload, during member boot up this error message is seen on member console.<br><br>2. ACL's applied on default VLAN(with scale) need to be part of the configuration.<br><br>3. Reload the device with the ACL configuration. After the reload the device may fail to program some ACL filters into Hardware TCAM. |
| Workaround | 1. Ensure that before reload of the system, ACL configuration is removed.<br>2. After reload, apply the ACL configuration. The TCAM will program the ACL's as expected. |
| Recovery | Remove the ACL corresponding to the failed ACL Id and add again |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180643 |
|---|---|
| Symptom | MACSec sessions between ICX 7650 and MLX has traffic drops when replay protection configuration does not match. |
| Condition | Connect ICX 7650 10G Fiber links to MLX<br>Configure replay protection in ICX 7650 to be different from MLX, such as disable on MLX and out-of-order on ICX 7650. |
| Workaround | Configure similar replay protection option in both ICX 7650 and MLX. |
| Recovery | Configure similar replay protection option in both ICX 7650 and MLX. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - MACsec - Media Access Control security |

| Issue | FI-180631 |
|---|---|
| Symptom | When scaled VXLAN overlay gateway configuration is deleted, it MAY not get deleted completely. |
| Condition | This issue MAY be seen when VXLAN overlay gateway (having below scaled configuration) is deleted<br><br>1. Many VLANs are mapped to VNIs i.e. more than 64 Vlan mapped to VNI<br>2. Multiple sites are configured i.e. more than 8 Tunnels/Sites.<br>3. Mapped VLANs are extended to multiple sites. |
| Workaround | Delete all the sites (one at a time) from the VXLAN overlay gateway, before deleting the VXLAN overlay gateway.<br><br>1). Remove site configuration one at a time.<br>2). This burdens CPU, so the system needs time for the CPU to come back to low, so wait for 30-60 sec for the system to settle down. Before removing next site.<br>3). Remove overlay-gateway in the end. |
| Recovery | Save the configuration and reload the switch. Once the switch boots up with partial VXLAN overlay gateway configuration, delete the VXLAN overlay gateway. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180625 |
|---|---|
| Symptom | During ISSU, in member units sometime we get L3 error messages and ISSU Aborts. |
| Condition | ISSU operation in 8070x Patch release on a router image on stacking or SPX system may exposed this problem. It due to a very narrow timing issue during ISSU due to which for some VE interface we get error message when member unit reloads and joins back. This in-turn causes ISSU to Abort. |
| Workaround | Reload of the system will required with the New image if the problem is seen on a system. |
| Recovery | Reload of the system will required with the New image. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180605 |
|---|---|
| Symptom | Clear command issued from enable prompt can result in inconsistent standby state in stack configurations.<br>For example, the following command<br>Router#clear ipv6 ospf<br>will only clear OSPF state on the Active unit. The Standby unit will maintain the old OSPF state. |
| Condition | This behavior exists since day-one and can be seen on all ICX images and platforms when in stacking configuration. |
| Workaround | In stacking configurations, to clear state or statistics on Active and Standby, the clear command should be issued from config prompt on the Active unit<br>For example, the following command<br>Router(config)#clear ipv6 ospf<br>executed on the Active unit will clear OSPF state on the Active as well as the Standby unit. |
| Recovery | Issuing the clear command from the config prompt will trigger a clear on all units of the stack and restore the system to a consistent state.<br>For example, if<br>Router#clear ipv6 ospf<br>left the Standby unit in an inconsistent state,<br>Router(config)#clear ipv6 ospf<br>when executed on the Active unit will clear OSPF state on the Active as well as the Standby unit and restore consistency. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-179991 |
|---|---|
| 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 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180553 |
|---|---|
| Symptom | PoE powersupply is shown as regular powersupply during bootup in active unit. |
| Condition | clear syslog, reload the device, "show log" output |
| Workaround | No Workaround |
| Recovery | None. |
| Probability | |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | |

| Issue | FI-180520 |
|---|---|
| Symptom | When a TLS connection is established to a Syslog server, two syslog messages will be seen for the Syslog server's certificate being successfully validated. There is no functional impact to this.<br>For example, when establishing a TLS connection between a TLS Client J-ICX7250-48-HPOE and the Syslog server associated with the trust point TLS-LINUX, the following messages will be seen.<br>SYSLOG: <14> Nov  1 16:28:08 J-ICX7250-48-HPOE PKI: Certificate validation for trustpoint TLS-LINUX success<br>SYSLOG: <14> Nov  1 16:28:08 J-ICX7250-48-HPOE PKI: Certificate validation for trustpoint TLS-LINUX success |
| Condition | The duplicate Syslog messages are always seen when the PKI validation of the TLS server's certificate is successful. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180510 |
|---|---|
| Symptom | When multiple PDs are connected and disconnected simultaneously multiple times and also if the available power is not sufficient for powering all the PDs, ICX might land into an issue of HW to SW configuration mismatch causing power to be not release on some ports like below.<br><br>3/1/17 On    Off       0    15400 n/a    n/a     3 n/a |
| Condition | Power might not get released on some ports when all PDs are multiple times disconnected and reconnected in a single shot. This scenario is unlikely with real PDs where all disconnect and reconnect at same instance. Issue was reported with Sifo test equipment. |
| Workaround | configure "no inline power" and then "inline power" on the ports where the issue is seen. |
| Recovery | The issue is caused due to high number of outstanding requests to the PoE controller overflowing the request queue.<br><br>configure "no inline power" and then "inline power" on the ports where the issue is seen. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-180466 |
|---|---|
| Symptom | When RSA private key file and ssl certificate are downloaded, it succeeds. However, the Active unit displays successful download but the Standby unit wrongly displays error message. |
| Condition | On ICX stack devices, on successful downloaded of RSA private key and ssl certificate shows success download in active unit but in standalone throws error. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | |

| Issue | FI-180434 |
|---|---|
| Symptom | With Default MACSec configuration between ICX 7650 and ICX 7450 or ICX 6610, traffic is not passing encrypted and protocol failures are observed. |
| Condition | 1. Default macsec session will have frame validation disabled. When frame-validation is disabled this issue will be seen<br><br>2. When mka group is configured with frame validation disabled, then also this issue will be seen.<br><br>3. Observed during interop of ICX 7650 with ICX 7450 or ICX 6610. |
| Workaround | Avoid using default macsec policy when connecting ICX 7650 with ICX 7450, ICX 6610 or MLX.<br>(or)<br>Create a MKA group with frame validation strict and apply it while enabling macsec for a port when connecting to other devices |
| Recovery | Create a MKA group with frame validation strict and apply it while enabling MACsec for a port when connecting to other devices |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | Security - MACsec - Media Access Control security |

| Issue | FI-180290 |
|---|---|
| Symptom | Sometimes on the ICX7000 series switches when the unexpected reload happens in the very rare case scenario, the stack trace is not seen indicating the reason for the system reload. The probability of this issue is very low. |
| Condition | This issue was observed on ICX7150, ICX7250, ICX7450 products when the switch reloads unexpectedly due to some corner case scenario. |
| Workaround | None |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-179715 |
|---|---|
| Symptom | Removing an ACL on the lag interface which has IPSG configured throws error in scaled/boundary tests. |
| Condition | On FastIron device, when ACL is applied and IPSG configured with maximum entries on lag interface. Then trying to remove acl configuration is not success and it throws error. It is removed in hardware not in software configuration. |
| Workaround | Issue seen only if maximum hardware resource or scaled entries reaches not on other scenarios. We can reduce the entries and it works fine. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | Security - IP Source Guard |

| Issue | FI-177386 |
|---|---|
| Symptom | Mac Authentication failure messages are getting printed in console for stack mac address. |
| Condition | The switch uses the stack MAC Address from the main unit for the mac authentication instead of end host mac. |
| Workaround | |
| Recovery | Not Applicable. |
| Probability | |
| Found In | FI 08.0.30 |
| Technology/ Technology Group | Security - 802.1x Port-based Authentication |

| Issue | FI-179449 |
|---|---|
| Symptom | On ICX7450 switch stack when the stack failover is done then in some rare cases the port state becomes inconsistent in the output of switch CLI. For example the port could be physically up but it shows up as Down in the switch CLI output like "show interface" when this command is issued from Active or Standby unit |
| Condition | This issue happens rarely on ICX7450 stack when the stack failover followed by a switch over . This issue happens rarely when port is changed from untagged to tagged configuration. |
| Workaround | None |
| Recovery | Recovery procedure is to disable and enable the port, the issue does not have any functional impact. |
| Probability | |
| Found In | FI 08.0.60 |

| Issue | FI-179167 |
|---|---|
| Symptom | Sometime the Bosch camera which is a POE PD devcie does not get powered up after connecting it to ICX7150 stacking standby unit and reloading the stack. This issue happens very rarely and it is a corner case. In this case the port state mismatch is observed between stacking Active and the Standby where the Active shows port status as Down and Standby port status is shown as Up |
| Condition | This issue happens in a very rare case when Bosch camera PD device is connected to the ICX7150 POE port on the stacking standby unit afer the stack reload is performed |
| Workaround | None |
| Recovery | Recovery procedure is to reload the particular stacking unit or the entire stack |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-179025 |
|---|---|
| Symptom | On ICX7750 when the cable is connected on the ports which are pre-configure to auto-lacp then the newly connected port comes up, goes down and then comes up again quickly. This port flap is observed only once during cable plug-in and after that the port works fine. This issue is observed only with auto-lacp and not with dynamic or static LAG |
| Condition | This issue is observed on ICX7750 ports when the port is configured for auto-lacp and then the cable is connected into the port to bring the link up |
| Workaround | There is no workaround as the port comes up after one flap and then works properly |
| Recovery | |
| Probability | |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-178663 |
|---|---|
| Symptom | GRE Tunnel (and potentially IP Unicast) Traffic forwarding via PE port is not getting redirected to new port even if alternative port available when PE goes down, traffic recovers when PE joins back, resulting is traffic loss even if there is alternative path. |
| Condition | GRE Tunnel (and potentially IP Unicast) Traffic egressing on a SPX PE Port and doing ISSU/HA operation resulting in temporary PE detach during that operation. |
| Workaround | Customer are advised to have PE connected to multiple CB via CB uplink spx-lag before performing switchover or failover to avoid PE Detach. For ISSU or any PE detach condition there is no workaround. |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-177856 |
|---|---|
| Symptom | Traffic forwarding based on the newly added rules fails after switchover and failover |
| Condition | - Openflow groups & flows configurations present in the system<br>- Trigger being a switchover or failover and during this period the groups get deleted by the controller, which would be missed by the device, as the new Active is still not connected to the OF Controller.<br>- After completion of the switchover/failover and Openflow purge timer expiry if the above added rules/groups are tried to be added again by the controller the same would fail. |
| Workaround | None |
| Recovery | None |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-177848 |
|---|---|
| Symptom | Applying an ACL on an interface with PBRv4/PBRv6 does not throw error when Hardware resources are full |
| Condition | Applying ACL on an interface with PBR |
| Workaround | To add new filter free up space by deleting existing ACL rules |
| Recovery | To add new filter free up space by deleting existing ACL rules |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-177843 |
|---|---|
| Symptom | Tunnel establishment fails for less than 5 tunnels and hence there is a data traffic forwarding on those tunnels fails. |
| Condition | 1) A device having a IPSec conifguration with more 40 IPSec tunnels<br>2) The authentication mechanism for IKE is PKI.<br>3) The IKE peer is same for all 40 tunnels<br>4) The PKI certificate is also the same.<br>5) Switchover or failover operation performed with the above configuration. |
| Workaround | Configuartion of IKE keepalive timer to 10 seconds. |
| Recovery | Clear IKE session of the the particular tunnel will recover the tunnel and its traffic after the condition occurs. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-177595 |
|---|---|
| Symptom | In rare circumstances, when ICX7650 boots up, a hardware initialization failure could trigger an additional reboot with the following error message - "FATAL ERROR: Failed in HW init hence rebooting". |
| Condition | In rare circumstances, when ICX7650 boots up, a hardware initialisation failure could trigger additional reboots. In this defect scenario, initialisation of 10GF port fails. |
| Workaround | No workaround available. |
| Recovery | No recovery needed. System recovers from the hardware initialization failure by rebooting automatically. |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-177056 |
|---|---|
| Symptom | High CPU of about 50% for 60 seconds on the new active after a switch over command provided by the user. This high CPU is seen only with BGP configuration over IPV6 IPSec tunnel configuration present in the device. |
| Condition | IPSec V6 tunnels configured in the device with BGP running over the tunnel and stack switch over trigger results in a high CPU of about 50% . |
| Workaround | None |
| Recovery | High CPU persists for about 60 seconds and comes back to normal with no functional impact. |
| Probability | |
| Found In | FI 08.0.70 |

| Issue | FI-176874 |
|---|---|
| Symptom | On ICX7150 switch when the user triggers reverse manifest operation by plugging in the external USB to switch and pressing the status button and if at the same time the supportsave operation is also going on in background due to user triggered CLI then sometimes the output of "show inline power" command is shown on console |
| Condition | This issue happens on ICX7150 switch when user connects the external USB to switch and triggers the reverse manifest operation by pressing the status button and at the same time the user triggers the supportsave operation from console CLI |
| Workaround | This is a message display issue and does not have any functional impact. The workaround to avoid this message is to not do the supportsave CLI and reverse manifest operation at the same time |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-175768 |
|---|---|
| Symptom | When ICX7150 is configured as a port extender in switch port extender setup then some of the ICX7150 flash file information is not correctly displayed at control bridge ICX7750 when the "show flash" command is issued from there. This issue happens for some of the ICX7150 in a switch port extender setup and this is a display issue, there is no functionality impact due to this issue |
| Condition | This issue happens sometimes when ICX7150 is working as a port extender in switch port extender setup and the "show flash" command is issued from control bridge to know the flash file content of ICX7150 unit |
| Workaround | There is no workaround. This issue happens only sometimes and there is no functionality impact due to this |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-168996 |
|---|---|
| Symptom | On ICX7150 when the system got reloaded due to the unexpected exception in the kernel, debug log messages are not stored in the flash. |
| Condition | This issue occurs in the very rare cases when system automatically reloads due to unexpected kernel exception. |
| Workaround | None |
| Recovery | |
| Probability | |
| Found In | FI 08.0.70 |
| Technology/ Technology Group | |

| Issue | FI-113814 |
|---|---|
| Symptom | User ACLs not getting applied correctly impacting traffic treatment through an interface that is authenticated with Flexauth. This can be observed when Flexauth User authentication succeeds on ports of standby and member units in a stack when PBR is already configured on the port. |
| Condition | The issue is observed in the following conditions. 1. PBR is enabled on the interface. 2. A user is attempting to get authenticated on the same member or standby     port with Radius returned ACL attribute. |
| Workaround | None |
| Recovery | 1. Remove PBR configuration on the interface with #no ip policy route-map <name of the map> 2. Clear Flexauth session with #clear macauth session eth <port> or clear dot1x session eth <port> 3. Users needs to be authenticated again |
| Probability | Low |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-120843 |
|---|---|
| Symptom | User ACLs do not get programmed for clients connected on stack member ports during flexible authentication with 'filter-strict-security disabled'. Hence traffic flow through this port will get impacted. |
| Condition | Observed under following conditions: 1. Strict security mode is disabled with 'no filter-strict-security enable' 2. User is authenticated with flexauth on the stack member port |
| Workaround | None |
| Recovery | enable 'filter-strict-security' and re-authenticate the users by using clear dot1x sessions and clear macauth sessions. |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-118277 |
|---|---|
| Symptom | Member port in a stack transitions to disabled state, after clearing dot1x session with radius returned mac-filter. |
| Condition | This issue is observed in the following conditions: 1. Authenticate dot1x user with radius returned mac-filter. 2. Clear the dot1x session and re-authenticate the session. |
| Workaround | None |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-120406 |
|---|---|
| Symptom | On ICX7xxx switch stack when we have port added or removed from a virtual LAG and the new standby unit gets elected due to older standby unit being removed or crashed then sometime the MRP state of interface LAG changes from pre-forwarding to forwarding to blocking |
| Condition | This happens sometimes on ICX7xxx switch stack when the MRP is configured on the VLAG and the interfaces are added or removed from the VLAG |
| Workaround | No workaround, the port state settles down to right state |
| Recovery | None |
| Probability | High |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-118189 |
|---|---|
| Symptom | Reload of stack results in few empty IP Source guard related Hardware rule entries corresponding to rules on standby ports. This could impact traffic from hosts corresponding to the non programmed entries. |
| Condition | Seen after a reload of stack with scaled IPSG clients (>700) on a standby port and greater than 2000 clients in the system. |
| Workaround | None |
| Recovery | At times reload of standby will help to recover but this is not deterministic. |
| Probability | Low |
| Found In | FI 08.0.61 |
| Technology/ Technology Group | |

| Issue | FI-114133 |
|---|---|
| Symptom | With ICX7750 router image, CPU usage is always around 3% even though system is idle and incase of switch image CPU usage remains around 1%. It is cosmetic issue and doesn't have any functional impact. |
| Condition | It is observed in ICX7750 when there is no configuration present and system is idle. |
| Workaround | None |
| Recovery | None |
| Probability | Medium |
| Found In | FI 08.0.60 |
| Technology/ Technology Group | |

| Issue | FI-110268 |
|---|---|
| Symptom | dot1x session with mac filter with deny is getting authenticated, hence users traffic will be permitted instead of blocking it. |
| Condition | This issue is observed in the following conditions: 1. configure mac filter '1' with deny action with destination as any. 2. Authenticate dot1x user with radius returned mac-filter 1 |
| Workaround | None |
| Recovery | None |
| Probability | Medium |
| Found In | FI 08.0.50 |
| Technology/ Technology Group | |