SOFTWARE UPGRADE GUIDE

RUCKUS FastIron Software Upgrade Guide, 09.0.10

Supporting FastIron Software Release 09.0.10

Part Number: 53-1005726-02
Publication Date: 15 February 2022

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

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 products, and customers and partners with active support contracts.

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

What Support Do I Need?

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

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

Open a Case

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

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

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

Self-Service Resources

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

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

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

Document Feedback

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

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

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

For example:

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

RUCKUS Product Documentation Resources

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

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

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

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About this Document

What's new in this document

NOTE

FastIron releases 09.0.00, 09.0.00a, and 09.0.10 are no longer available for download due to the recent discovery of a critical defect. RUCKUS recommends upgrading to FastIron release 09.0.10a for all ICX switches currently running any of the afore-mentioned releases. Refer to *TSB 2022-001 – FastIron 09.0.00 and 09.0.10 - Risk of Filesystem Corruption* on the Technical Support Bulletins page for more details.

All the software features supported in FastIron release 09.0.00, 09.0.00a, and 09.0.10 remain available and supported in FastIron release 09.0.10a.

TABLE 2 Summary of enhancements in FastIron release 09.0.10

Feature	Description	Location
Updates to address defects	Updates on content throughout to address defects.	All chapters.
Minor editorial updates	Minor editorial updates were made throughout the Configuration Guide.	All chapters.

Supported Hardware

This guide supports the following RUCKUS products:

- RUCKUS ICX 7850 Switch
- RUCKUS ICX 7650 Switch
- RUCKUS ICX 7550 Switch
- RUCKUS ICX 7450 Switch
- RUCKUS ICX 7250 Switch
- RUCKUS ICX 7150 Switch

For information about what models and modules these devices support, refer to the hardware installation guide for the specific product family.

Software Upgrade and Downgrade

Software Upgrade Procedure Overview

You can upgrade FastIron software in several ways: through a manual step-by-step process, through a manifest file, or through a Unified FastIron Image (UFI).

1. Preliminary checks. For any upgrade, review the information in General Considerations for Upgrade to or Downgrade from FastIron 09.0.00 or Later on page 12 and then follow the instructions in Initial Steps on page 13 to determine the current software versions, license requirements, and instructions on where to download the software.

   Unless configured, syslogs do not persist across reloads.

2. Upgrade the software. For a step-by-step upgrade, refer to Upgrade Process on page 27.

   NOTE
   Beginning with the FastIron 08.0.90 release, UFI image copy is the recommended software upgrade method for both standalone devices and traditional stacks.

   NOTE
   Beginning with the FastIron 08.0.90 release, all new hardware platforms, starting with ICX 7850 devices, support only UFI images for software upgrade.

   NOTE
   For a stack, you can perform a full manual upgrade for each unit, or you can download the software as described in Upgrade Process on page 27 followed by an In-service software upgrade for the stack as described in In-service Software Upgrade on page 45. Be sure to check ISSU Limitations and Considerations on page 45 before performing an In-service software upgrade.

General Considerations for Upgrade to or Downgrade from FastIron 09.0.00 or Later

Prepare for the Upgrade

Because of the many software design and CLI changes implemented in FastIron release 09.0.00, downgrading to a previous release is complex and may produce unexpected results.

IMPORTANT REMINDER
Be sure you have backed up your previous startup configuration before you begin any upgrade or downgrade process.

Before upgrading to FastIron 09.0.00 or a later release, RUCKUS strongly recommends these steps:

- Make a backup copy of the ICX startup configuration (the startup-config file). This copy will be used if a downgrade to a previous release is necessary. If you have made changes to the running configuration, you may also want to save a copy of the running-config file.

  The following example saves a copy of a FastIron 08.0.95 startup configuration and a running configuration and stores them on the TFTP server, identified by its IP address.

  ```
  ICX# copy startup-config tftp 10.176.198.42 old-8095-cfg
  ICX# Upload startup-config to TFTP server done.
  ICX# copy running-config tftp 10.176.198.42 old-8095-run-cfg
  ICX# Upload running-config to TFTP server done.
  ```

  NOTE
  A FastIron 09.0.00 or later startup-config file does not parse properly for a pre-09.0.00 release due to design changes. When you downgrade, configuration changes, including user account configuration and stack configuration, among others, will be lost.

- Consult the FastIron release notes and user documentation for the current release about significant software design changes that may need to be taken into consideration.

  NOTE
  If you are upgrading to FastIron release 09.0.00 or a later release and the ICX device contains the configuration **service password-encryption sha1**, any users who are configured with sha1 encryption are removed during the upgrade.

Transition to cli timeout

The **cli timeout** command is introduced in FastIron 09.0.00 and replaces the **ip ssh idle-time**, **telnet timeout**, and **console timeout** commands. The following rules apply when converting timer configuration from earlier releases on upgrade to FastIron 09.0.00:

- The default value for the **cli timeout** command is 2 minutes, which applies if none of the replaced commands has prior configuration. After 2 minutes, by default, a console, telnet, or ssh session times out.
- Previously, the default for console timeout was 0, which meant the console session never timed out. Starting with FastIron 09.0.00, if you do not want sessions to time out, you must set the **cli timeout** value to 0.
- On upgrade to FastIron 09.0.00 or a later release, the **cli timeout** value is acquired from previous configuration in the following order of priority:
  - **ip ssh idle-time** configuration
  - **telnet timeout** configuration
  - **console timeout** configuration

Initial Steps

NOTE
You must upgrade to the boot code that supports the current release. Refer to "Image File Names" in the release notes for detailed information.

RUCKUS recommends that you always use the manifest file for any image upgrade or downgrade.

If you are upgrading from FastIron release 08.0.80 to release 08.0.90 or later, RUCKUS recommends using SCP to transfer files.

Determining the Current Flash Image Version

To determine the current flash image version of the device, enter the **show flash** command at any level of the CLI.

The following **show flash** output is for releases prior to FastIron 08.0.90.

```
device# show flash
Stack unit 1:
  Compressed Pri Code size = 31768772, Version:08.0.30T213 (SPR08030.bin)
  Compressed Sec Code size = 31768772, Version:08.0.30T213 (SPR08030.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.06T215
  Code Flash Free Space = 1602994176
Stack unit 3:
  Compressed Pri Code size = 31768772, Version:08.0.30T213 (SPR08030.bin)
  Compressed Sec Code size = 31768772, Version:08.0.30T213 (SPR08030.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.06T215
  Code Flash Free Space = 1604464640
Stack unit 4:
  Compressed Pri Code size = 31768772, Version:08.0.30T213 (SPR08030.bin)
  Compressed Sec Code size = 31768772, Version:08.0.30T213 (SPR08030.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.06T215
  Code Flash Free Space = 1588183040
```

Determining the Current Flash and Boot Image Versions

To determine the current boot and flash image versions installed on a device, enter the **show version** command at any level of the CLI.

```
device# show version
  Copyright (c) 1996-2016 Brocade Communications Systems, Inc. All rights reserved.
    UNIT 3: compiled on Jan 21 2019 at 23:28:08 labeled as SPR08030
      (31768772 bytes) from Primary SPR08030.bin
        SW: Version 08.0.30T213
    UNIT 1: compiled on Jan 21 2019 at 23:28:08 labeled as SPR08030
      (31768772 bytes) from Primary SPR08030.bin
        SW: Version 08.0.30T213
    UNIT 4: compiled on Jan 21 2019 at 23:28:08 labeled as SPR08030
      (31768772 bytes) from Primary SPR08030.bin
        SW: Version 08.0.30T213
      Compressed Boot-Monitor Image size = 786944, Version:10.1.06T215 (spz10106)
  HW: Stackable ICX7450-48
  Internal USB: Serial #: 9900314061200173
      Vendor: ATP Electronics, Total size = 1919 MB
==========================================================================
UNIT 1: SL 1: ICX7450-48F 48-port Management Module
      Serial  #:CYS3333K006
      License: ICX7450_L3_SOFT_PACKAGE   (LID: eauIIIImFFL)
      License Compliance: ICX7450-PREM-LIC-SW is Compliant
.
.
The system : started=warm start   reloaded=by "reload"
My stack unit ID = 3, bootup role = active
```

Determining the Current Licenses Installed

Use the **show version** or the **show license** command to display the licenses installed on the device.

```
ICX7150-C12-SW1# show version
Copyright (c) Ruckus Networks, Inc. All rights reserved.
UNIT 1: compiled on Jul 28 2021 at 05:45:11 labeled as SPR09000
(33554432 bytes) from Secondary SPR09000.bin (UFI)
SW: Version 09.0.00T213
Compressed Primary Boot Code size = 786944, Version:10.1.18T225 (mnz10118)
Compiled on Mon Jul 13 03:53:29 2020

HW: Stackable ICX7150-C12-POE
==========================================================================
UNIT 1: SL 1: ICX7150-C12-2X1G POE 12-port Management Module
Serial #:FEK3239N0R6
Software Package: ICX7150_L3_SOFT_PACKAGE
Current License: 2X10GR
P-ASIC 0: type B160, rev 11 Chip BCM56160_B0
==========================================================================
UNIT 1: SL 2: ICX7150-2X1GC 2-port 2G Module
==========================================================================
UNIT 1: SL 3: ICX7150-2X10GF 2-port 20G Module
==========================================================================
1000 MHz ARM processor ARMv7 88 MHz bus
8 MB boot flash memory
2 GB code flash memory
1 GB DRAM
STACKID 1 system uptime is 39 day(s) 3 hour(s) 5 minute(s) 42 second(s)
The system started at 22:59:46 Central Fri Aug 20 2021

The system : started=cold start
ICX7150-C12-SW1#

ICX7150-C12-SW1# show license
Unit License Name L3 Premium Port Speed Upgrade Speed Ports MACsec
1 2X10GR Yes Yes 10G 2 NA
```

Obtaining Software Licenses

NOTE
For complete instructions on how to generate a license, refer to the *RUCKUS FastIron Software Licensing Guide*.

1. If required, generate a new license from the License Management page on the RUCKUS Support website. If you are upgrading to a different type of image that uses a different license from the one already installed on the device, generate a separate license file.
2. Download the required software images for the target release from the Software Downloads page on the RUCKUS Support website. For the list of software image files available for FastIron 08.0.xx, refer to the release notes for the specific release.

Upgrade Considerations for Licensed Features

Upgrading or downgrading to a different FastIron release can affect the availability of licensed features on the system. Review the following upgrade considerations before upgrading.

Upgrading from FastIron 08.0.70 or Earlier to 09.0.00 or Later for the ICX 7150, ICX 7250, ICX 7450, and ICX 7650

When upgrading directly from FastIron 08.0.70 or earlier releases to 09.0.00 or later releases, all pre-existing licensed features and in some cases access lists (ACLs) will be lost. To prevent the loss of licensed features and ACLs, perform the upgrade in two steps:

1. First, upgrade to the 08.0.80f non-UFI version. Upgrade the respective boot image also, and save the configuration with the write memory command.
2. Second, upgrade to 08.0.90 UFI or later release. When upgrading to the UFI version, the boot image will be upgraded automatically.

The upgrade path is 08.0.70 or prior -> 08.0.80f (non-UFI) –> 09.0.00 or later (UFI).

NOTE
This upgrade consideration applies only when the ICX 7150, ICX 7250, ICX 7450, and ICX 7650 platforms are upgraded from 08.0.70 or earlier releases. It does not apply to upgrades from 08.0.80f or later.

Upgrading from FastIron 08.0.70 and Earlier Releases to 09.0.00 or Later

Beginning in FastIron 08.0.80, the Self-Authenticated Upgrade (SAU) licensing model was implemented on all the RUCKUS ICX platforms. When upgrading from FastIron 08.0.70 or earlier releases, existing software feature licenses on the device will be converted to SAU licenses. The original XML licenses are preserved on the system in case the switch is downgraded to an earlier version that requires them.

Refer to the following topics for important considerations when upgrading:

- Upgrade Considerations for the Layer 3 Premium License on page 15
- Upgrade Considerations for Ports on Demand Licenses on page 16
- Upgrade Considerations for MACsec Licenses on page 17

Upgrade Considerations for the Layer 3 Premium License

In FastIron 08.0.70 and earlier releases, Layer 3 Premium licenses on the ICX 7250 and ICX 7450 were implemented as XML licenses. Beginning with FastIron 08.0.80, all Layer 3 Premium licenses are Self-Authenticated Upgrade (SAU) licenses.

Upgrading a System Without a Layer 3 Premium License from FastIron 08.0.70 or Earlier Releases

Layer 3 Premium licensed features are not available until the user has enabled the Layer 3 Premium SAU license. Without the Layer 3 Premium license, the Layer 3 licensed features cannot be used. This is a change in behavior for the ICX 7250 and ICX 7450; in releases prior to FastIron 08.0.80, licensed Layer 3 features could be enabled before a license was installed.

In an upgrade from FastIron 08.0.70 or earlier releases to FastIron 08.0.80 or later releases, the system enables the Layer 3 Base license package automatically, which means all Layer 3 premium features are disabled.

However, if the system does not have a Layer 3 Premium XML license and Layer 3 Premium features are configured, these L3 features will be lost after the upgrade. In order to avoid losing Layer 3 configurations, perform one of the following actions before or after the upgrade:

- Before upgrading the system, check the license compliance status. Purchase and install the Layer 3 Premium XML license on the device if needed. Always back up the configuration, and keep a backup of all license files.
- Before upgrading the system, back up the configuration. After the upgrade, enable the Layer 3 Premium SAU license and copy the configuration back to the system.
- After upgrading the system, immediately enable the Layer 3 Premium SAU license, but do not save the configuration, and then reload. After the system is back up, the Layer 3 Premium configuration should be back as it was before the upgrade.

NOTE
In this case, the running configuration is lost, but the Layer 3 premium configuration remains in the startup configuration as long as the user does not enter the **write mem** command after the upgrade.

In a stacking configuration, if Layer 3 licensed features are required then a valid Layer 3 Premium license must be installed on all members of the stack.

If the active unit has an XML Layer 3 Premium license installed, the Layer 3 Premium configuration should remain the same after the upgrade, but member units without a Layer 3 Premium XML license will enter a non-operational state. To prevent member units from becoming non-operational, copy the Layer 3 Premium XML license to relevant units before the upgrade, or enable the Layer 3 Premium SAU license on relevant units after the upgrade.

If the active unit does not have a Layer 3 Premium XML license, the configuration of any premium Layer 3 features will be lost after the upgrade. Use one of the three preceding methods to prevent the loss of or to recover the Layer 3 configuration.

ICX Device with an Existing Layer 3 Premium XML License

If there is an existing Layer 3 Premium XML license on the device, the system will automatically enable the Layer 3 Premium SAU license upon upgrade to 08.0.80, and Layer 3 feature configuration will be retained. All Layer 3 features will function as before the upgrade.

All XML license files will be preserved in case the device is loaded with a non-SAU license image (that is, in case of a downgrade).

Upgrade Considerations for Ports on Demand Licenses

In FastIron 08.0.70 and earlier releases, Ports on Demand (PoD) licenses on the ICX 7250 were implemented as XML licenses. Beginning with FastIron 08.0.80, all PoD licenses are Self-Authenticated Upgrade (SAU) licenses.

Upgrading an ICX 7250 Without an XML PoD License

Without a PoD license, all the licensed ports on an ICX 7250 have 1-Gbps speed. After an upgrade to FastIron 08.0.80 or later releases, these ports will continue to have 1-Gbps speed. If a 10-Gbps port is needed after the upgrade, you can enable the PoD SAU license for the 2x10G or 8x10G option.

When upgrading from FastIron 08.0.90 to a release later than FastIron 08.0.95x, a working 10-Gbps optic on an ICX 7250 without a PoD license no longer works because the configuration default is 1-Gbps.

Upgrading an ICX 7250 With an Existing XML PoD License

When an ICX 7250 with an existing PoD XML license is upgraded to FastIron 08.0.80 or later releases, the system automatically converts the PoD XML license to the corresponding PoD SAU license.

An upgrade to 08.0.80 has no impact on a stacking system.

When a user sets the PoD SAU license, the system looks at the existing XML license. If the option selected is of an equal or lower capacity to thePoD XML license, the SAU license is enabled. If an option with a higher capacity that the PoD XML license is selected, the SAU license is not enabled and the system displays a message instructing you to delete the PoD XML license before enabling the SAU license.

All XML license files will be preserved in case the device is downgraded to FastIron 08.0.70 or earlier release.

Upgrade Considerations for MACsec Licenses

In FastIron 08.0.70 and earlier releases, MACsec licenses were implemented as XML licenses. Beginning with FastIron 08.0.80, all MACsec licenses are Self-Authenticated Upgrade (SAU) licenses.

Upgrading an ICX 7450 or ICX 7650 Without an Existing MACsec License

A MACsec license is required to enable MACsec encryption on a port. When upgrading from FastIron 08.0.70 or earlier releases to FastIron 08.0.80 or later releases, if there is not an existing MACsec XML license on the switch, the MACsec SAU license will not be enabled after the upgrade.

Upgrading an ICX 7450 or ICX 7650 With an Existing MACsec License

When an ICX 7450 or ICX 7650 with an existing MACsec XML license is upgraded to FastIron 08.0.80 or later releases, the system automatically converts the MACsec XML license to the corresponding SAU license.

An upgrade to FastIron 08.0.80 or later releases has no impact on a stacking system.

Downgrading from 09.0.00 or Later Releases

When downgrading from FastIron 09.0.00 or later releases to 08.0.70 or earlier releases on an ICX 7250, ICX 7450, or ICX 7650, licensed features will be lost unless there is a pre-installed XML license on the device. Licensed features that have an XML license will be retained during the downgrade.

Downgrading from 09.0.00 or later to a release between 08.0.80 and 08.0.95 will not impact license features.

Upgrade Considerations for ACLs

This section describes the software upgrade changes related to access control lists (ACL). For more detailed information, refer to the *RUCKUS FastIron Security Configuration Guide*.

Upgrading from FastIron 08.0.70 or Earlier to 09.0.00 or Later for the ICX 7150, ICX 7250, ICX 7450, and ICX 7650

When upgrading directly from FastIron 08.0.70 or earlier releases to 09.0.00 or later releases, all pre-existing licensed features and in some cases access lists (ACLs) will be lost. To prevent the loss of licensed features and ACLs, perform the upgrade in two steps:

1. First, upgrade to the 08.0.80f non-UFI version. Upgrade the respective boot image also, and save the configuration with the write memory command.
2. Second, upgrade to 08.0.90 UFI or later release. When upgrading to the UFI version, the boot image will be upgraded automatically.

The upgrade path is 08.0.70 or prior -> 08.0.80f (non-UFI) –> 09.0.00 or later (UFI).

> **NOTE**
> This upgrade consideration applies only when the ICX 7150, ICX 7250, ICX 7450, and ICX 7650 platforms are upgraded from 08.0.70 or earlier releases. It does not apply to upgrades from 08.0.80f or later.

MAC ACLs

When upgrading from a previous major release to FastIron 08.0.95 or a later release, all the existing MAC filters and their bindings in the startup configuration are migrated to MAC ACLs.

MAC filters defined by the **mac filter** command in releases prior to FastIron 08.0.95 that are bound to a particular physical interface or LAG with the **mac filter-group** command are converted into MAC ACLs, which are configured from FastIron 08.0.95 using the **mac access-list** command. The **mac access-list** command allows permt and deny filter statements to be created in MAC ACL configuration mode. The filters in a MAC ACL will appear in the same order as defined in the MAC filters.

> **NOTE**
> MAC ACLs permit and deny statements have a syntax similar to IP ACLs. For more information, refer to the *RUCKUS FastIron Command Reference Guide*.

An existing MAC filter that is not in any binding group is translated and added into a default MAC ACL. The **mac filter-group** command, used for binding MAC filters on an interface and LAG in releases prior to FastIron 08.0.95 has been replaced with the **mac access-group** command. The **mac access-group** command binds MAC ACLs to a physical interface, LAG, VLAN, and so on. The MAC filter functionality remains intact after an upgrade. Beginning with FastIron 08.0.95, the **mac filter** and **mac filter-group** commands are deprecated.

ACL Logging Upgrade Considerations

In FastIron 08.0.95 and later releases, the **acl-logging** command for IPv4 and **logging-enable** command for IPv6 are replaced by the **logging enable** command. ACL logging is configurable only at the binding level and is used in conjunction with the **log** keyword at the filter level for IPv4, IPv6, and MAC ACLs.

After upgrade to FastIron 08.0.95 or a later release, the following changes occur if ACL logging is enabled.

- IPv4 ACL: If logging is enabled for an interface before upgrade, then logging will be enabled for all the existing ACLs on the interface to which they are bound to and their ingress and egress directions after the upgrade.
- IPv6 ACL: If logging is enabled for an IPv6 ACL and the interface to which it is bound before upgrade, then logging will be enabled for all bindings of the existing ACLs in both the ingress and egress directions after the upgrade.
- MAC ACL: If MAC filter logging is enabled on global level before upgrade, then log option will get added to all MAC ACL rules after the upgrade. Also, if logging is enabled for a filter group binding to an interface before upgrade, then logging will be enabled for the respective bindings corresponding to the filter group and interface combination in the ingress direction after the upgrade.

  > **NOTE**
  > On RUCKUS ICX 7150, ICX 7550, ICX 7650, and ICX 7850 devices, ACL logging is not supported for ACLs applied to outbound traffic.

ACL Accounting Upgrade Considerations

ACL accounting will be enabled by default for all filters. In FastIron 08.0.95 and later releases, the **enable-accounting** command has been modified to **enable accounting**.

After upgrade to FastIron 08.0.95 or a later release, the following changes occur for ACL accounting:

- IPv4 ACL: If accounting is enabled for an IPv4 ACL before upgrade, then it is enabled for all the filters that belong to that ACL after the upgrade.
- IPv6 ACL: If accounting is enabled for an IPv6 ACL before upgrade, then it is enabled for all the filters that belong to that ACL after the upgrade.
- MAC ACL: If accounting is enabled for a MAC filter before upgrade, then it is enabled for any MAC ACL that contains the filter after the upgrade.

The ACL accounting configuration of the MAC filter will migrate seamlessly during the upgrade. The accounting configuration for MAC filters that are not bound to any interface will be lost during upgrade and must be configured again for any resulting MAC ACL.

ACL- Related Changes When Upgrading to FastIron 08.0.95 or Later

The following table offers details regarding an upgrade to a FastIron 08.0.95 or later image with respect to ACLs.

Functionality	FastIron 08.0.92	FastIron 08.0.95 or Later
ACL MIB	• ACL MIBs are indexed using ACL ID. • Supported MIBs for ACLs bound to VE and interfaces only.	• ACL MIBs are indexed using ACL name. • MIB support for ACLs bound to VLAN, LAG, and VPORT (VLAN + port). • MIB is not supported for ACLs on VE. • You must switch to new ACL MIBs for RUCKUS ICX devices running FastIron 08.0.95 and later releases.
IPv4 ACL filter	A number of well-known protocol name options are supported. A number of well-known TCP or UDP port name options are supported.	Well-known protocol name options of an IPv4 Extended ACL filter configuration are reduced to a few commonly used names. However, any protocol configuration is allowed by specifying the corresponding protocol number. TCP or UDP application port name options of an IPv4 Extended ACL filter configuration are reduced to a few commonly used application port names. However, any application can be configured by specifying the corresponding port number.
IPv6 ACL filter	A number of well-known protocol name options are supported. A number of well-known TCP or UDP port name options are supported.	Well-known protocol name options of an IPv6 ACL filter configuration are reduced to a few commonly used names. However, any protocol configuration is allowed by specifying the corresponding protocol number. TCP or UDP application port name options while configuring an IPv6 ACL filter are reduced to a few commonly used application port names. However, any application can be configured by specifying the corresponding port number.
MAC filter configuration	MAC filter configuration using the **mac filter** command is supported.	The MAC filter group configuration is auto converted to a named MAC ACL in FastIron 08.0.95. The ACL logging or mirroring or accounting configuration in the MAC filter is migrated seamlessly. The **mac filter** command at the global level and the **mac filter-group** command at the interface level are deprecated and replaced by the **mac access-list** command with underlying filter statements beginning in FastIron 08.0.95. The accounting configuration for MAC filters that are not bound to any interface will be lost during upgrade and must be configured again for any resulting MAC ACL.

Functionality	FastIron 08.0.92	FastIron 08.0.95 or Later
IPv4 ACL binding	The following configurations are supported in FastIron 08.0.92: • ACL binding at the VE level in a router image. • • The per-VLAN ACL configuration in a switch image. • • ACL binding at the selective port of a VE in a router image.	ACL binding to a VLAN on both the switch and router image is supported. The ACL binding configuration at the VE level is converted to a VLAN configuration. The ACL binding on the per- vlan and selective port of a VE is converted to the binding of a selective port in a VLAN.
IPv6 ACL binding	ACL binding at the VE level in a router image is supported.	The binding of an ACL to a VLAN in both the switch and router image is supported. The ACL binding configuration at the VE level is converted to a VLAN configuration. Beginning with FastIron 08.0.95, the binding command **ipv6 traffic-filter** is changed to the **ipv6 access-group** command.
MAC filter binding	MAC filter binding is supported.	The MAC filter binding group forms a MAC ACL and is bound to an interface, much like an IP ACL. The MAC filter functionality remains intact. Beginning with FastIron 08.0.95, the **mac-filter group** command is modified to the **mac access-group** command.
ACL Accounting	Accounting is enabled at the ACL level for IPv4 and IPv6 ACLs, and enabled at the filter level for MAC ACLs.	Accounting is configurable at an ACL level. Accounting is applied for all the filters on all interfaces to which the ACL is bound. ACL accounting is enabled by default. The **enable accounting** command has been introduced. The auto-migration uses the new **enable accounting** command.
ACL Logging	Logging is enabled at the interface level for IPv4 ACLs and at the ACL level for IPv6 ACLs, and enabled at filter and filter-group level for MAC ACLs.	Logging is configurable only at the binding level using the **logging enable** command in conjunction with the **log** keyword at the filter level for IPv4, IPv6, and MAC ACLs. If ACL logging is enabled in an earlier release, ACL logging is enabled automatically under resulting ACL binding after the upgrade process.
DSCP or PCP Remarking	The DSCP or PCP remarking configuration at the global level is supported.	In FastIron 08.0.95 and later releases, the DSCP or PCP remarking configuration at the global level is not supported, even though it was configured in a previous release. You can configure DSCP or PCP at the interface level, where DSCP actions will be merged with the user ACLs bound on the interface.
Per-port-per-VLAN	The per-port-per-VLAN configuration is supported.	The **enable acl-per-port-per-vlan** command is deprecated in FastIron 08.0.95. By default, all ports are enabled with per-port-per-VLAN.
ACL Policy	The **acl-policy** command and the **suppress-acl-seq** commands are supported. These commands are used during the downgrade process to FastIron 08.0.50 or releases prior to FastIron 08.0.50.	The **acl-policy** command and **suppress-acl-seq** commands are deprecated in FastIron 08.0.95.
ACL on ARP	ACL ID is not mandatory.	In FastIron 08.0.95 and later releases, an ACL ID is mandatory to configure an ACL on ARP. Enter an ACL number to specify the ACL to be used for filtering. If you have configured an ACL ARP without an ACL ID in an earlier release, the system will lose the configuration during the upgrade process.

Functionality	FastIron 08.0.92	FastIron 08.0.95 or Later
ND-packet hop-limit check	The ND hop-limit configuration is configured using the **enable nd hop-limit** command under IPv6 ACL.	The ND hop-limit functionality is enabled by default. The **ipv6 nd ra-hop-limit** and **enable nd hop-limit** commands are deprecated. Checking for ND packets with a hop limit less than 255 helps protect against denial of service (DoS) attacks. The **enable nd-hop-limit** command is deprecated beginning with FastIron 08.0.95.
Traffic Policy	The **cir** keyword is not supported in the configuration.	The **traffic-policy rate-limit adaptive** and **traffic-policy rate-limit fixed** commands are modified to add a new **cir** keyword. The rate can be specified as either packets or bytes.
DDoS	DDoS configuration on a virtual Ethernet interface is supported.	DDoS configuration at the VLAN level in a router image is allowed. During the upgrade process, the DDoS configuration at the VE level in a router image is applied to the VLAN in FastIron 08.0.95 and later releases.
DDoS configuration on a tagged or dual mode interface in a switch image	DDOS configuration is supported on a virtual Ethernet interface on router images and on tagged or dual mode interfaces in a switch image in pre-08.0.95 release.	During the upgrade process,DDOS configuration under tagged or dual mode interface in a switch image will be lost. You have to re-configure the same configuration under VLAN in switch images in FastIron 08.0.95 and later releases.
DHCPv4 and DHCPv6 snooping on VLANs of a VLAN group	DHCPv4 or DHCPv6 snooping must be enabled on all the VLANs in a VLAN group.	DHCPv4 and DHCPv6 snooping on VLANs of a VLAN group is not supported. You will lose the configuration during the upgrade process.
IP Source Guard (IPSG)	IPSG configuration at the VE level in a router image, and at per-port-per-VLAN in a switch image is supported.	IPSG configuration at the VE level and at per-port-per-VLAN will be migrated to a VLAN with the selective port option.
IPSG and ingress IPv4 User ACL (UACL) for the same port	IPSG and ingress IPv4 UACL configuration for the same port can be configured together at the interface level or at the VE level or per-vlan level.	If a port has both IPSG and UACL configuration together at any level, the upgrade process does not take place, and you will lose the UACL configuration. A warning message is displayed for the problem during bootup in FastIron 08.0.95 and later releases.
System default values and **system-max** commands for Static DAI and DHCP snooping	The system default values for Static Dynamic ARP Inspection (DAI) entries is 512 and for DHCP snooping is 8192. However, these default values can be changed for Static DAI and DHCP snooping using the **system-max max static-inspect-arp-entries** and **system-max max max-dhcp-snoop-entries** commands, respectively.	The **system-max** commands for Static DAI and DHCP snooping are deprecated beginning in FastIron 08.0.95, and the configurations are lost during the upgrade process. The new system default value for Static DAI is 6000 and for DHCP snooping is 32768.
DHCP snooping flash update interval configuration	The **ip dhcp snooping flash-update-interval** command is supported.	The **ip dhcp snooping flash-update-interval** command is deprecated beginning in FastIron 08.0.95 and the system will lose the configuration during the upgrade process.
System default values	The system default value depends upon the hardware.	The system default value depends upon the hardware. System default values for the ICX 7550 include the following values: Maximum configurable filters the device supports (IPv4 and IPv6 ACLs): 8192 Maximum configurable filters per ACL (either IPv4 or IPv6 ACLs): 2048 MAC filter statements per ACL: 256 MAC filter statements per stack: 3072

Functionality	FastIron 08.0.92	FastIron 08.0.95 or Later
Authentication filter	MAC filter ID can be passed to the **authentication auth-filter** command configured in interface configuration mode	The **authentication auth-filter** command is deprecated and replaced by the **authentication filter** command. A MAC ACL filter has to be provided to this command instead of MAC ACLs. The MAC ACL filter supports source MAC address filters only.
Maximum VLAN support with User ACL clients	There is no limit.	FastIron 08.0.95 and later releases support up to 512 VLANs to bind different clients having the same functionality. For example, features such as IPSG, DAI, and DHCP snooping can be enabled on 512 VLANs. A functionality enabled on more than 512 VLANs will lose the configuration during migration.
DHCP snooping or DAI or IPv6 Network Interface Identifier enabled on VLAN.	DHCP snooping or DAI or Network Interface Identifier enabled on a VLAN without ports does not allocate hardware resources.	DHCP snooping or DAI or Network Interface Identifier enabled on a VLAN without ports allocates hardware resources for each VLAN for each Control Bridge (CB) unit. If TCAM space is full, enabling DHCP snooping or DAI or NDI on a VLAN without ports causes functionality failures during migration.
DHCP snooping database	The DHCP snooping database file name format is **dhcpsnoop.db**.	The DHCP snooping database file name format is **icx_dhcp_snoop.db**. Remove all entries from the DHCP binding database using the **clear dhcp** and **clear ipv6 dhcp6 snoop** commands before the downgrade process to a release prior to FastIron 08.0.95.

NOTE

On an ICX 7850 device, if you migrate to FastIron 08.0.95 or a later release from a FastIron 08.0.92 configuration that contains an IPv4 egress ACL applied to a virtual interface, the two TCAM rules originally programmed for the ACL (one ACL rule and one implicit deny rule) are programmed as four TCAM rules in the target release configuration, where the ACL will be applied at the VLAN level; that is, two rules for the ACL and two rules for the implicit deny rule.

On an ICX 7850 device, if you migrate from FastIron 08.0.92 to FastIron 08.0.95 or a later release, the rules created for an IPv6 egress ACL applied to a virtual interface multiply. For example, if you created the original IPv6 egress ACL with one rule, the ACL is programmed as four rules in TCAM for the FastIron 08.0.92 configuration; that is, one IPv6 ACL rule and three implicit rules. In the resulting configuration for the target release, the IPv6 ACL is applied at the VLAN level, and a total of eight rules will be created in TCAM; that is, two ACL rules and six implicit rules.

Upgrade Considerations for the ICX7150-C08P

Beginning with FastIron 08.0.92, the ICX7150-C08P supports a new BCM53443 SoC chipset. The new chipset offers no functionality changes.

NOTE

FastIron 08.0.91 and earlier builds cannot be downloaded on the ICX7150-C08P and ICX7150-C08PT with the BCM53443 SoC chipset.

The **show version** command output is modified to reflect the BCM53443 SoC chipset.

```
ICX 7150-C08P# show version

Copyright (c) Ruckus Networks, Inc. All rights reserved.
UNIT 1: compiled on Jul 12 2019 at 00:05:03 labeled as SPS08092_Q1
(28631220 bytes) from Primary SPS08092_Q1.bin (UFI)
SW: Version 08.0.92_Q1T211
Compressed Primary Boot Code size = 786944, Version:10.1.17T225 (mnz10117b4)
Compiled on Tue Jul  2 10:26:13 2019
HW: ICX7150-C08-POE
==========================================================================
UNIT 1: SL 1: ICX7150-C08-2X1G POE 8-port Management Module
```

```
      Serial  #:FMF3209Q00J
      Software Package: BASE_SOFT_PACKAGE
      P-ASIC  0: type 8443, rev 11  Chip BCM53443_B0
==========================================================================
UNIT 1: SL 2: ICX7150-2x1GF 2-port 2G Module
==========================================================================
 1000 MHz ARM processor ARMv7 88 MHz bus
 8192 KB boot flash memory
 2048 MB code flash memory
 1024 MB DRAM
STACKID 1  system uptime is 7 day(s) 3 hour(s) 11 minute(s) 4 second(s)
The system started at 00:02:58 GMT+00 Thu Jan 01 1970
The system : started=cold start
```

Upgrade Considerations for Stacks

Read the following section before upgrading a stack from a pre-08.0.90 release to FastIron 08.0.90 or later and before downgrading from FastIron 08.0.90 or a later release to a pre-08.0.90 release. Certain stack configuration behaviors have changed in FastIron release 08.0.90, and new commands have been introduced to assist with upgrades and downgrades. For additional information on stacking changes, refer to the *RUCKUS FastIron Stacking Configuration Guide*.

In pre-09.0.00 to 09.0.00 upgrade process, ICX 7150 stack configured with 4k VLANS takes around 35 minutes to be stack ready after reload. It includes time taken to boot up, complete config parsing, and config sync to standby unit. For a standalone ICX 7150, it takes around 24 minutes to complete config parsing after reload.

Changes to Upgrade and Downgrade for Stacking from FastIron Release 08.0.90

The stacking port format is different beginning with FastIron 08.0.90. The change in format creates upgrade and downgrade issues.

Upgrading a Stack to FastIron Release 08.0.90 or Later from Earlier Releases

Upgrades from earlier releases to FastIron 08.0.90 or a later release are seamless. FastIron 08.0.90 and later releases recognize the old format and parse startup-config flash to convert the configuration to the new format. After upgrade, if you enter the **write memory** command to save the configuration, the new format is stored to startup-config flash.

In the following example, an ICX 7450 stack is upgraded to FastIron 08.0.90 from FastIron 08.0.80 startup-config flash. The user has not yet used the **write memory** command. Output for the **show configuration** command shows that the FastIron 08.0.80 startup-config flash remains in the old format. The command output for the **show running-config** command displays the runtime configuration in the new format.

```
ICX7450-48P Router# show configuration
!
Startup-config data location is flash memory
!
Startup configuration:
!
ver 08.0.80 <-- old 08.0.80 release startup-config flash
!
stack unit 1
module 1 icx7450-48p-poe-management-module
module 2 icx7400-xgf-4port-40g-module
module 3 icx7400-qsfp-1port-40g-module
module 4 icx7400-qsfp-1port-40g-module
priority 128
default-ports 1/2/1 1/2/3
stack-trunk 1/2/1 to 1/2/2
stack-trunk 1/2/3 to 1/2/4
stack-port 1/2/1 1/2/3
stack unit 2
module 1 icx7450-48p-poe-management-module
module 2 icx7400-xgf-4port-40g-module
```

```
module 3 icx7400-qsfp-1port-40g-module
module 4 icx7400-qsfp-1port-40g-module
priority 128
default-ports 2/2/1 2/2/3
stack-trunk 2/2/1 to 2/2/2
stack-port 2/2/1 2/2/3
stack enable
stack mac 609c.9f2a.97e0

ICX7450-48P Router# show running-config
Current configuration:
!
ver 08.0.90
!
stack unit 1
module 1 icx7450-48p-poe-management-module
module 2 icx7400-xgf-4port-40g-module
module 3 icx7400-qsfp-1port-40g-module
module 4 icx7400-qsfp-1port-40g-module
priority 128
stack-trunk 1/2/1 to 1/2/2
stack-trunk 1/2/3 to 1/2/4
stack unit 2
module 1 icx7450-48p-poe-management-module
module 2 icx7400-xgf-4port-40g-module
module 3 icx7400-qsfp-1port-40g-module
module 4 icx7400-qsfp-1port-40g-module
priority 128
stack-trunk 2/2/1 to 2/2/2
stack-port 2/2/3
stack enable
stack mac 609c.9f2a.97e0
```

Downgrading a Stack from FastIron 08.0.90 or 08.0.95 to a Pre-08.0.90 Release

A standalone or active controller parses the startup-config flash to read the stacking ports for the entire stack. A release prior to FastIron 08.0.90 does not understand startup-config flash content generated by FastIron 08.0.90 or later releases. As a result, if you try to downgrade from FastIron 08.0.90 or later to a pre-08.0.90 release, the stack may break. FastIron 08.0.90 attempts to overcome the need to downgrade by saving and recovering the original startup-config flash.

In FastIron 08.0.90, when the **write memory** command is used, the system renames the startup-config flash "pre-8090-startup-backup" if it has been generated from a pre-08.0.90 release. You can view the contents of the saved file using the **show pre-8090-startup-backup** command.

> **NOTE**
> When a stack downgrades to a pre-08.0.90 release from recovered pre-08.0.90 startup-config flash, it loses all configuration changes made under FastIron 08.0.90 or a later release.

Every unit, including a stack member, has a startup-config file, and every unit renames the startup-config as the backup file when the **write memory** command is used.

If you no longer need the pre-8090-startup-backup file, you can delete it using the **erase pre-8090-startup-backup** command. This command erases the pre-8090-startup-backup file in every unit in the stacking system. You may no longer need the older backup file if you are certain you will not have to downgrade the system or if you have made many configuration changes with the FastIron 08.0.90 or later release installed, making the backup file obsolete.

When a system running FastIron 08.0.90 or a later release detects that it is about to reload to a pre-08.0.90 release, the system tries to recover the backup file. A message is displayed asking for confirmation before recovering the file with a warning that all changes made with the current release will be lost.

```
ICX7450-48P Router# boot system flash secondary
Are you sure? (enter 'y' or 'n'): y
Warning! the startup-config is 8.0.90 or later, but you are reloading to a pre-8090 image.
The system will use the pre-8090-startup-backup file to reload and lose all 8.0.90 changes.
```

```
(You can type "show pre-8090-startup-backup" to see its content.)
Do you want to reload ? (enter 'y' or 'n'): y
Reload using pre-8090-startup-backup file.
```

NOTE

Beginning with FastIron release 9.0.00, you are not prompted with a warning regarding saving the startup-config file. Only the following warning is displayed:

```
Running Config data has been changed. Do you want to continue  the reload without
saving the running config? (enter 'y' or 'n'):
```

NOTE

In contrast, the **reload yes** and **boot system flash secondary yes** commands do not require confirmation. The following example shows the system response when the **boot system flash secondary yes** command is entered.

```
ICX7450-48P Router# boot system flash secondary yes
Reload using pre-8090-startup-backup file.
T=8m11.3: Halt and reboot
```

When a system is upgraded to FastIron 08.0.90 or later and then downgraded to a pre-08.0.90 release, the results of the downgrade differ, depending on the situation. The following cases describe specific situations and the expected results. The scenarios in the following tables apply to a standalone unit or a stack.

TABLE 3 Stack Downgrade Scenarios

Situation	Result
The user never uses a **write memory** command when running FastIron 08.0.90.	The downgrade is seamless.
The user does not change any configuration but uses the **write memory** command when running FastIron 08.0.90.	The downgrade is fine. The system recovers the backup file before reloading to a pre-08.0.90 release.
The user makes configuration changes while running FastIron 08.0.90 and uses the **write memory** command.	The downgrade loses all configuration changes made under FastIron 08.0.90. The system recovers the backup file that does not contain the changes.

Switchover or failover does not affect these downgrade scenarios. For example, you may perform a switch-over to change the active controller and then reload. The recovery result is the same as a reload without changing the active controller.

There are a few cases where recovery does not work.

TABLE 4 Scenarios where Stack Downgrades Cannot Be Performed

Situation	Result
The user reloads the system by powering down.	The system cannot recover the backup file before reloading.
The standalone or active controller does not have a startup-config flash file generated by any pre-08.0.90 release.	Downgrade is not possible.

NOTE

It is recommended that you copy the running configuration to a file before downgrading. You can do this using the **copy running-config** command to copy the configuration to different locations such as a USB disk file or a tftp server, or you can simply enter the **show running-config** command and then copy the output and paste it into a computer file.

NOTE

If you don't have a pre-08090-startup-backup file (which can be checked with the **show pre-8090-startup-backup** command), or you have many configuration changes to the 08.0.90 release or a later release and you need to downgrade to a pre-08.0.90 release, you must manually edit the 08.0.90 configuration to create a pre-08.0.90 format.

Downgrading a Stack to a pre-09.0.00 Release

NOTE
RUCKUS recommends that you establish a console connection with all stack units prior to the downgrade.

The major format change for stacking in the FastIron 09.0.00 release is the inclusion of the keyword **ethernet** before port IDs (for example, **stack-port ethernet 1/2/1**) in the **stack-port**, **stack-trunk**, **multi-stack-port**, and **multi-stack-trunk** commands.

To downgrade to a pre-09.0.00 release in 08.0.9x format, copy back to the ICX device the old startup-config file you saved previously. The following example downgrades an ICX 7550 device by copying the file named saved_startup_08095 from the server at the specified IP address and saving it as startup-config.

```
ICX7550-48ZP Router# copy tftp startup-config 10.176.131.99 saved_startup_08095
Parameter Validation Successful
Startup Config Download started
Startup Config Download Done
Startup Config sync complete
Startup Config Write Done
Startup Config Download Complete
```

If you have backed up the configuration and you use the correct saved startup-config file, the stack should remain intact. However, if the stack breaks for any reason, such as a power failure, use the recovery procedure in the following section to re-establish the stack and stacking connections.

If ncessary, contact the Technical Assistance Center for support. Refer to Contacting RUCKUS Customer Services and Support on page 5 for contact information and for details on opening a ticket.

How to Recover a Broken Stack after a Downgrade from FastIron 09.0.00 or Later

Downgrading from FastIron 09.0.00 or a later release is complex and may produce unexpected results. Refer to the previous section for recommended steps before downgrading.

If a stack has broken following a downgrade from a more recent release to an 08.0.9x release, you can use the following procedure to recover the stack.

When the stack breaks on downgrade, the stack boots up without stack ports as shown in the following example.

```
ICX7550-48 Router# show running-config
Current configuration:
!
ver 08.0.95c
!
stack unit 1
 module 1 icx7550-48-port-management-module
 module 2 icx7550-qsfp-2port-80g-module
 priority 128
stack unit 2
 module 1 icx7550-48-port-management-module
 module 2 icx7550-qsfp-2port-80g-module
 module 3 icx7600-xgf-4port-40g-module
stack unit 3
 module 1 icx7550-48p-port-management-module
 module 2 icx7550-qsfp-2port-80g-module
 module 3 icx7600-xgf-4port-40g-module
stack mac 4cb1.cd20.36be
```

NOTE
Depending on the target downgrade release, the **show running-config** command output may show different results. In some releases, default stack-ports may be present.

Perform the following steps to recover the stack.

1. Connect to the active controllers' local console.
2. In privileged EXEC mode, enter the **configure terminal** command.

```
ICX7550-48 Router#  configure terminal
ICX7550-48 Router(config)#
```

3. In global configuration mode, enter the **stack unit** command followed by the unit ID of the active controller (1 in the following example).

```
ICX7550-48 Router(config)# stack unit 1
ICX7550-48 Router(config-unit-1)#
```

4. Configure the original stack-port(s) or stack-trunk(s) for the active controller.

   In the following example, two stack-ports are configured.

```
ICX7550-48 Router(config-unit-1)# stack-port 1/2/1
ICX7550-48 Router(config-unit-1)# stack-port 1/2/2
```

   NOTE
   You do not need to update the stack-ports or stack-trunks for the other stack units. The active controller will learn the connections from the members as they join the stack.

5. Return to global configuration mode, and enter the **stack enable** command.

```
ICX7550-48 Router(config-unit-1)# exit
ICX7550-48 Router(config)# stack enable
```

   As soon as stacking is enabled, the active controller will attempt to form a stack. However, the original standby controller may not join the stack because it may have become a standalone unit.

6. Use one of the following options to recover the standby controller.
   - Access the standby controller's local console, and configure the unit's original stack-port(s) or stack-trunk(s).
   - From the active controller, enter the **stack interactive-setup** command, and choose Option **3** when prompted to discover the standby unit as part of the stack.

```
ICX7550-48 Router(config)# exit
ICX7550-48 Router# stack interactive-setup
You can abort stack interactive-setup at any stage by <ctrl-c>
0: quit
1: change stack unit IDs
2: discover and convert new units (no startup-config flash) to members
3: discover and convert existing/new standalone units to members
2&3 can also find new links and auto-trunk or convert chain(s) to ring.

Please type your selection: 3
Probing topology to find standalone units...
```

7. Once the stack forms, enter the **write memory** command to save the running-configuration.

Upgrade Process

NOTE
Before upgrading the software on a RUCKUS ICX device, refer to General Considerations for Upgrade to or Downgrade from FastIron 09.0.00 or Later on page 12, Initial Steps on page 13, and other relevant considerations included in this chapter. For a stacking system, also refer to Changes to Upgrade and Downgrade for Stacking from FastIron Release 08.0.90 on page 23.

Software images for all RUCKUS ICX devices can be uploaded and downloaded between flash modules on the device and a TFTP, SCP, HTTPS, or USB module on the network.

RUCKUS ICX devices have two flash memory modules:

- Primary flash: The default local storage device for image files and configuration files.
- Secondary flash: A second flash storage device. You can use secondary flash to store redundant images for additional booting reliability or to preserve one software image while testing another one.

Only one flash device is active at a time. By default, the primary image becomes active when you reboot the device.

The following methods are available to upgrade your RUCKUS ICX device.

- Trivial File Transfer Protocol (TFTP): Use TFTP to copy an image from a TFTP server onto a flash module.
- Secure Copy Protocol (SCP): Use SCP to copy images to and from a host (recommended).
- Hypertext Transfer Protocol Secure (HTTPS): From FastIron release 08.0.80, you can use HTTPS, which requires a server that supports HTTP over TLS.
- Universal Serial Bus (USB): From FastIron release 08.0.30, you can use a USB device that contains the appropriate files and is connected to a standalone unit or the active controller in a stack.

Software Mandatory Upgrade Steps from a Pre-08.0.80 Non-UFI Version to a 09.0.00 or Later UFI Version

Upgrading from a Pre-08.0.80 non-UFI version to a FastIron 09.0.00 or later UFI version is a two-step upgrade process. For example, if you want to upgrade a stacking unit or a standalone device from FastIron 08.0.70 to FastIron 09.0.00 or later, complete the following steps.

1. Download the 08.0.80f non-UFI using one of the transfer methods listed in Table 3, and reboot the device with the 08.0.80f image using the **boot system flash primary** command. The system uses the 08.0.80f image. Save the running configuration to startup configuration using the **write memory** command.

   NOTE
   The above step is mandatory as it migrates the configured Access Control list (ACL) configurations without sequence numbers to the new ACL format. The system will otherwise lose the previously configured ACL configuration without sequence numbers while upgrading from a pre-08.0.90 non-UFI version to a UFI version.

2. Copy the 09.0.00 or later UFI to the primary flash partition using the same method, and reboot the device again.

   NOTE
   The **show version** command might display boot code mismatch message after performing the above upgrade step.

   Re-copy the 09.0.00 or later UFI to the secondary flash partition to avoid boot image mismatch.

   NOTE
   Download the 08.0.95 image using one of the transfer methods listed in Table 3 to upgrade a device from FastIron 08.0.80 release to FastIron 09.0.10 release.

TABLE 5 File Transfer Method and Commands Required

Transfer Method	Commands
TFTP	1a) device# copy tftp flash 10.177.16.144 SPR08080f.bin primary 1b) device# copy tftp flash 10.177.16.144 spz10114.bin bootrom 2a) device# copy tftp flash 10.177.16.144 SPR09000ufi.bin primary 2b) device# copy tftp flash 10.177.16.144 SPR09000ufi.bin secondary or 1) device# copy tftp system-manifest 10.176.220.51 FI08080f_Manifest.txt all-images-primary 2a) device# copy tftp system-manifest 10.176.220.51 FI09000_Manifest.txt primary 2b) device# copy tftp system-manifest 10.176.220.51 FI09000_Manifest.txt secondary
SCP	1a) device# copy scp flash 10.176.132.13 SPR08080f.bin primary 1b) device# copy scp flash 10.176.132.13 spz10114.bin bootrom 2a) device# copy scp flash 10.176.132.13 SPR09000ufi.bin primary 2b) device# copy scp flash 10.176.132.13 SPR09000ufi.bin secondary
HTTPS [FastIron 08.0.80 and later]	1a) device# copy https flash 10.176.132.132 SPR08080f.bin primary 1b) device# copy https flash 10.176.132.132 spz10114.bin bootrom 2a) device# copy https flash 10.176.132.132 SPR09000ufi.bin primary 2b) device# copy https flash 10.176.132.132 SPR09000ufi.bin secondary
USB	1a) device# copy disk0 flash SPR08080f.bin primary 1b) device# copy disk0 flash spz10114.bin bootrom 2a) device# copy disk0 flash SPR09000ufi.bin primary 2b) device# copy disk0 flash SPR09000ufi.bin secondary

NOTE

The system will lose the auth-filter configuration during the upgrade process to FastIron 09.0.00 or a later release or on reload with a 08.0.80 release. Re-configure the **authentication-filter** command after the system reloads with the FastIron 09.0.00 or later image.

Loading the Flash Code using TFTP

1. a. Copy the 08.0.80f non-UFI from the TFTP server into flash memory using the **copy tftp flash** command.

```
ICX7250-48 Router# copy tftp flash 10.177.16.144 SPR08080f.bin primary
Load to buffer (8192 bytes per dot)
.....................................................................
.....................................................................
TFTP to Flash Done.
```

b. Copy the bootrom images using the following command.

```
ICX7250-48 Router# copy tftp flash 10.177.16.144 spz10114.bin bootrom
Load to buffer (8192 bytes per dot)
.....................
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(65536 bytes per dot)...
............
TFTP to Flash Done.
```

c. Enter the **show flash** command to verify the image and uboot files have been installed in the primary partition flash.

```
ICX7250-48 Router# show flash
Stack unit 1:
  Compressed Pri Code size = 29829112, Version:08.0.80fT213 (SPR08080f.bin)
  Compressed Sec Code size = 29515932, Version:08.0.70fT213 (SPR08070f.bin)
  Compressed Boot-Monitor Image size = 786432, Version:10.1.14T215
  Code Flash Free Space = 1613783040
```

d. Reboot the device with the 08.0.80f image using the **boot system** command.

NOTE

Use the **boot system flash primary** command to boot the image from the primary flash memory.

```
ICX7250-48 Router# boot system flash primary
```

e. Enter the **show version** command to display the flash image running on the device.

```
ICX7250-48 Router# show version
Copyright (c) 2017 Ruckus Wireless, Inc. All rights reserved.
    UNIT 1: compiled on Apr  6 2020 at 22:40:21 labeled as SPR08080f
      (29829112 bytes) from Primary SPR08080f.bin
        SW: Version 08.0.80fT213
      Compressed Boot-Monitor Image size = 786944, Version:10.1.14T215 (spz10114)
       Compiled on Thu Nov 15 12:59:16 2018

  HW: Stackable ICX7250-48
==========================================================================
UNIT 1: SL 1: ICX7250-48 48-port Management Module
      Serial  #:DUJ3851L0CL
      Software Package: ICX7250_L3_SOFT_PACKAGE   (LID: fwlINKGnFen)
      Current License: l3-prem-8X10G
      P-ASIC  0: type B344, rev 01  Chip BCM56344_A0
==========================================================================
UNIT 1: SL 2: ICX7250-SFP-Plus 8-port 80G Module
==========================================================================
1000 MHz ARM processor ARMv7 88 MHz bus
8192 KB boot flash memory
2048 MB code flash memory
2048 MB DRAM
STACKID 1  system uptime is 2 minute(s) 41 second(s)
The system started at 04:27:55 GMT+00 Wed Jul 29 2020

The system : started=warm start   reloaded=by "reload"
```

2. a. Copy the 09.0.00 or later UFI from the TFTP server into flash memory using the **copy tftp flash** command.

```
ICX7250-48 Router# copy tftp flash 10.177.16.144 SPR09000ufi.bin primary

Load to buffer (8192 bytes per dot)
.....................................................
.....................................................
Processing the bundle image...
Flashing application image to Primary partition...

SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(65536 bytes per dot)...
.....................................................
Flashing bootrom image...

SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(65536 bytes per dot)...
............
Post processing bundle image...
Bundle image processed successfully
```

b. Save the running configuration to startup configuration using the **write memory** command.

```
ICX7250-48 Router# write memory
```

c. Reboot the device with the 09.0.00 or later UFI image using the **boot system flash primary** command.

```
ICX7250-48 Router# boot system flash primary
```

NOTE

The system does not support full functionality such as third-party packages (DHCPv6, HTTP, Python, and so on.) without a UFI update. If you stop the upgrade process after the reboot without downloading the UFI, the following warning message is displayed on the console.

```
WARNING: FI image is not booted from UFI. Please download UFI image and reboot the system for
 full functionality.
```

NOTE

The **show version** command might display boot code mismatch message after performing the above upgrade.

d. Re-copy the 09.0.00 or later UFI from the TFTP to the secondary flash partition to avoid boot image mismatch.

```
ICX7250-48 Router# copy tftp flash 10.176.198.42 SPR09000ufi.bin secondary
Parameter Validation Successful
Image Download started

SYSLOG: <14> Sep 30 20:31:48 ICX7250-48 Router COPY IMAGE TO FLASH START
.................................................Image Download Done
Image Validation Started

SYSLOG: <14> Sep 30 20:33:05 ICX7250-48 Router COPY APPLICATION IMAGE FROM BUNDLE START

SYSLOG: <14> Sep 30 20:33:05 ICX7250-48 Router COPY BOOTROM IMAGE FROM BUNDLE START
Image Write Done
Image Download Complete
ICX7250-48 Router#
SYSLOG: <14> Sep 30 20:33:25 ICX7250-48 Router COPY BUNDLE IMAGE COMPLETED
```

e. Enter the **show version** command to display the flash image running on the device.

```
ICX7250-48 Router# show version

Copyright (c) Ruckus Networks, Inc. All rights reserved.
    UNIT 1: compiled on Jul 20 2021 at 22:56:24 labeled as SPR09000
      (32947884 bytes) from Primary SPR09000.bin (UFI)
        SW: Version 09000
      Compressed Primary Boot Code size = 786944, Version:10.1.18T215 (spz10118)
       Compiled on Mon Jul 13 08:53:15 2021
```

```
  HW: Stackable ICX7250-48
==========================================================================
UNIT 1: SL 1: ICX7250-48 48-port Management Module
      Serial  #:DUJ3851L0CL
      Software Package: ICX7250_L3_SOFT_PACKAGE   (LID: fwlINKGnFen)
      Current License: l3-prem-8X10G
      P-ASIC  0: type B344, rev 01  Chip BCM56344_A0
==========================================================================
UNIT 1: SL 2: ICX7250-SFP-Plus 8-port 80G Module
==========================================================================
1000 MHz ARM processor ARMv7 88 MHz bus
    8 MB boot flash memory
    2 GB code flash memory
    2 GB DRAM
STACKID 1  system uptime is 1 minute(s) 49 second(s)
The system started at 04:41:32 GMT+00 Wed Jul 29 2021

The system : started=warm start   reloaded=by "reload"
```

f. Enter the **show flash** command to verify the image and uboot files.

```
ICX7250-48 Router# show flash
Stack unit 1:
  Compressed Pri Code size = 33554432, Version:09.0.00T213 (SPR09000.bin)
  Compressed Sec Code size = 33554432, Version:09.0.00T213 (SPR09000.bin)
  Compressed Pri Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
  Compressed Sec Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
  Code Flash Free Space = 1492922368
Stack unit 2:
  Compressed Pri Code size = 33554432, Version:09.0.00T213 (SPR09000.bin)
  Compressed Sec Code size = 33554432, Version:09.0.00T213 (SPR09000.bin)
  Compressed Pri Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
  Compressed Sec Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
  Code Flash Free Space = 1496690688
ICX7250-48 Router#
```

When upgrading the flash image version, the image is automatically updated across all stack units. When upgrading from one major release to another (for example, from FastIron 08.0.90 to FastIron 09.0.00), make sure that every unit in the traditional stack has the same major code version. If you reboot the stack while units are running different code versions, the units cannot communicate.

Loading the Flash Code Using the Manifest Method

1. a. Copy the 08.0.80f non-UFI from the TFTP server into flash memory using the **copy tftp system-manifest** command.

```
ICX7450-48P Router# copy tftp system-manifest 10.176.220.51 FI08080f_Manifest.txt all-images-primary
You are about to download boot image and boot signature image as well,
ARE YOU SURE?(enter 'y' or 'n'): Error: Enter y/n or Y/N for confirmation
Y
ICX7450-48P Router#Flash Memory Write (8192 bytes per dot)
DOWNLOADING MANIFEST FILE Done.
ICX7450-48P Router#Flash Memory Write (8192 bytes per dot)
Automatic copy to member units: 2 3
COPY ICX7450 SIGNATURE TFTP to Flash Done
ICX7450-48P Router#Load to buffer (8192 bytes per dot)
Automatic copy to member units: 2 3
.....................................................................................................
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot).................
.....................................................................................................
Copy ICX7450 from TFTP to Flash Done
ICX7450-48P Router#Flash Memory Write (8192 bytes per dot)
Automatic copy to member units: 2 3
......
DOWNLOAD OF ICX7450 BOOT SIGNATURE Done
ICX7450-48P Router#Load to buffer (8192 bytes per dot)
Automatic copy to member units: 2 3
.........................
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per
dot).................
.....................................................................................................
.
ICX7450 Boot IMAGE COPY IS DONE
Manifest image download is complete, please reload the system
```

b. Enter the **show flash** command to verify the image and uboot files have been installed in the primary partition flash.

```
ICX7450-48P Router# show flash

Stack unit 1:
  Compressed Pri Code size = 29826604, Version:08.0.80fT213 (SPR08080f.bin)
  Compressed Sec Code size = 28584896, Version:08.0.70T211 (SPS08070.bin)
  Compressed Boot-Monitor Image size = 786432, Version:10.1.14T215
  Code Flash Free Space = 1604861952
Stack unit 2:
  Compressed Pri Code size = 29826604, Version:08.0.80fT213 (SPR08080f.bin)
  Compressed Sec Code size = 28584896, Version:08.0.70T211 (SPS08070.bin)
  Compressed Boot-Monitor Image size = 786432, Version:10.1.14T215
  Code Flash Free Space = 1588035584
Stack unit 3:
  Compressed Pri Code size = 29826604, Version:08.0.80fT213 (SPR08080f.bin)
  Compressed Sec Code size = 28584896, Version:08.0.70T211 (SPS08070.bin)
  Compressed Boot-Monitor Image size = 786432, Version:10.1.14T215
  Code Flash Free Space = 1605509120
```

c. Reboot the device with the 08.0.80f image using the **boot system flash primary** command. to boot the image from the primary flash memory.

```
ICX7450-48P Router# boot system flash primary
```

d. Enter the **show version** command to display the flash image running on the device.

```
ICX7450-48P Router# show version

Copyright (c) 2017 Ruckus Wireless, Inc. All rights reserved.
    UNIT 1: compiled on Apr  9 2019 at 03:20:17 labeled as SPR08080f
      (29826604 bytes) from Primary SPR08080f.bin
        SW: Version 08.0.80fT213
.
.
.
.
```

```
STACKID 1  system uptime is 12 minute(s) 20 second(s)
STACKID 2  system uptime is 8 minute(s) 45 second(s)
STACKID 3  system uptime is 8 minute(s) 43 second(s)
The system started at 16:15:10 Pacific Wed Sep 11 2019

The system : started=warm start   reloaded=by "reload"
My stack unit ID = 1, bootup role = active
```

2. a. Copy the 09.0.00 UFI from the TFTP server into flash memory using the **copy tftp system-manifest** command.

```
ICX7450-48P Router# copy tftp system-manifest 10.176.198.42 9000/FI09000_Manifest.txt primary
Flash Memory Write (8192 bytes per dot)
DOWNLOADING MANIFEST FILE   Done.
Manifest upgrade in progress...
Flash Memory Write (8192 bytes per dot)
COPY ICX7450 SIGNATURE TFTP to Flash Done
Load to buffer (8192 bytes per dot)
.........................................
Processing the bundle image...
Flashing application image to Primary partition...
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
.....................................................................................
Flashing bootrom image...

SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
.....................................................................................
Post processing bundle image...
Bundle image processed successfully

Copy ICX7450 from TFTP to Flash Done

Manifest file upgrade done, please reload the system
Copying the downloaded/created manifest file from ramfs to flash...
.
Copy Done.

ICX7450-48P Router# show flash
Stack unit 3:
  Compressed Pri Code size = 33554432, Version:09.0.00T213 (SPR09000.bin)
  Compressed Sec Code size = 29829112, Version:08.0.80fT213 (SPR08080f.bin)
  Compressed Boot-Monitor Image size = 786432, Version:10.1.20T215
  Code Flash Free Space = 1248391168
ICX7450-48P Router#
```

b. Save the running configuration to startup configuration using the **write memory** command.

```
ICX7450-48P Router# write memory
```

c. Reboot the device with the 09.0.00 UFI image using the **boot system flash primary** command.

```
ICX7450-48P Router# boot system flash primary
```

d. Re-copy the 09.0.00 manifest file to the secondary flash partition to avoid boot image mismatch.

```
ICX7450-48P Router# copy tftp system-manifest 10.176.198.42 09000/FI09000_Manifest.txt secondary
```

e. Enter the **show version** command to display the flash image running on the device.

```
ICX7450-48P Router# show version
  Copyright (c) Ruckus Networks, Inc. All rights reserved.
    UNIT 3: compiled on Jul 28 2021 at 05:45:11 labeled as SPR09000
      (33554432 bytes) from Primary SPR09000.bin (UFI)
        SW: Version 09.0.00T213
      Compressed Primary Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
       Compiled on Fri Apr 30 06:48:50 2021
!
!
```

Loading the Flash Code Using SCP

The new flash code must be placed on an SCP-enabled host to which the RUCKUS ICX device has access.

NOTE
Copying the manifest file using SCP is not supported.

1. a. Copy the flash code from the SCP-enabled host into the flash memory.

```
ICX7450-24P Router# copy scp flash 10.176.132.13 SPR08080f.bin primary

User name:root
Password:
Connecting to remote host......

Receiving data (8192 bytes per dot)
.................................
Automatic copy to member units:  1  4
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
Image copy completed
Primary Image file downloaded successfully.
SCP transfer to device completed
Outbound Connection Closed
```

b. Copy the flash code to bootrom.

```
ICX7450-24P Router# copy scp flash 10.176.132.13 spz10114.bin bootrom

User name:root
Password:
Connecting to remote host......

Receiving data (8192 bytes per dot)
.........................................................
Automatic copy to member units:  1  4
.....................................................................................................

SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...

Image copy completed
.....................................................................................
Done.
SCP transfer to device completed
Connection Closed
```

c. Save the running configuration to startup configuration using the **write memory** command.

```
ICX7450-24P Router# write memory
```

2. a. Reload the device and then immediately upgrade to the UFI.

```
ICX7450-24P Router# boot system flash primary
```

b. Re-copy the 09.0.00 or later UFI to the primary and the secondary flash partition to avoid boot image mismatch.

```
ICX7450-24P Router# copy scp flash 10.176.132.13 SPR09000ufi.bin primary
User name:root
Password:
Connecting to remote host......

Receiving data (8192 bytes per dot)
Image copy completed

ICX7450-24P Router# copy scp flash 10.176.132.13 SPR09000ufi.bin secondary
```

Using SCP to copy UFI images from an external device to an ICX device

The following example copies a FastIron 09.0.00 UFI image file from the SCP server to the primary flash memory.

```
[user@l42-icx-linux-80 Images]$ scp SPR09000ufinss.sig user@10.176.132.142:flash:primary
    Password: xxx
```

The following example copies a UFI image signature file from the SCP server to the flash memory.

```
[user@l42-icx-linux-80 Images]$ scp GZR10000_b308ufi.sig user@10.176.132.142:flash
    Password: xxx
```

Loading the Flash Code Using HTTPS

The HTTPS method for loading flash code is available for FastIron 08.0.80 and later releases.

1. a. Copy the flash code from the HTTPS to flash memory.

   ```
   ICX7450-48P Router# copy https flash 10.176.132.132 SPR08080f.bin primary
   ```

   b. Copy the flash code to bootrom.

   ```
   ICX7450-48P Router# copy https flash 10.176.132.132 spz10114.bin bootrom
   ```

   c. Save the running configuration to startup configuration using the **write memory** command.

   ```
   ICX7450-48P Router# write memory
   ```

2. a. Reload the ICX device and then perform the UFI upgrade.

   ```
   ICX7450-48P Router# boot system flash primary
   ```

   c. Re-copy the 09.0.00 or later UFI to primary and the secondary flash partition to avoid boot image mismatch.

   ```
   ICX7450-48P Router# copy https flash 10.176.132.132 SPR09000ufi.bin primary
   ICX7450-48P Router# copy https flash 10.176.132.132 SPR09000ufi.bin secondary
   ```

Loading the Flash Code Using USB

1. a. Copy the application image and the boot image to the flash from the USB.

   ```
   ICX7450-48P Router# copy disk0 flash SPR08080f.bin primary
   ICX7450-48P Router# copy disk0 flash spz10114.bin bootrom
   ```

   b. Save the running configuration to startup configuration using the **write memory** command.

   ```
   ICX7450-48P Router# write memory
   ```

2. a. Reload the device and immediately perform a UFI upgrade.

   ```
   ICX7450-48P Router# boot system flash primary
   ```

   b. Re-copy the 09.0.00 or later UFI to primary and the secondary flash partition to avoid boot image mismatch.

   ```
   ICX7450-48P Router# copy disk0 flash SPR09000ufi.bin primary
   ICX7450-48P Router# copy disk0 flash SPR09000ufi.bin secondary
   ```

   c. Enter the **show version** command to verify that the UFI image has loaded successfully.

Software Upgrade from a UFI to FastIron 09.0.00 or Later UFI Release

Upgrading from a UFI version to a FastIron 09.0.00 or later UFI version is a one-step upgrade process.

If you want to upgrade from a UFI version (for example, 08.0.92) to FastIron 09.0.00 or later, download the 09.0.00 or later UFI and use the **boot system flash primary** command to reload the device. Re-copy the 09.0.00 or later UFI to the secondary and the primary flash partition to avoid boot image mismatch.

TABLE 6 File Transfer Method and Commands Required

Transfer Method	Commands
TFTP	1a) device# copy tftp system-manifest 10.176.132.11 FI09000_Manifest.txt primary 1b) device# copy tftp system-manifest 10.176.132.11 FI09000_Manifest.txt secondary or 2a) device# copy tftp flash 10.176.132.11 SPR09000ufi.bin primary 2b) device# copy tftp flash 10.176.132.11 SPR09000ufi.bin secondary
SCP	device# copy scp flash 10.176.132.11 SPR09000ufi.bin primary device# copy scp flash 10.176.132.11 SPR09000ufi.bin secondary
HTTPS [FastIron 08.0.80 and later]	device# copy https flash 10.176.132.132 SPR09000ufi.bin primary device# copy https flash 10.176.132.132 SPR09000ufi.bin secondary
USB	device# copy disk0 flash SPR09000ufi.bin primary device# copy disk0 flash SPR09000ufi.bin secondary

Image download using USB

Beginning with FastIron 08.0.90, the system can be upgraded by downloading the manifest file in the USB drive.

When TFTP server access is not available, you can use the manifest file in the USB to download the images of a system. Manifest image download using USB is not supported for 08.0.80 and earlier releases. In earlier releases, USB image download was supported for standalone systems only. USB image download is supported on all ICX 7K hardware platforms.

The following actions must be performed to initiate the upgrade using the USB drive.

1. Plug in a valid USB drive (USB2 drives and backward-compatible USB3 drives) with the appropriate pre-loaded manifest files to the system.
2. Reload the unit with the USB drive plugged in.

   NOTE
   USB image download is not supported in FIPS mode.

Software upgrade using USB is not triggered in the following scenarios:

- If the USB drive is not detected during the bootup.
- When the USB drive is corrupted, not accessible, unmountable, or if there is no valid file system in the USB drive.
- If there is an existing configuration file in the system.

NOTE
The configuration file must be deleted from the system using the **erase startup-configuration** command. Image download using USB is not triggered if there is a configuration file in the system.

When the image is successfully copied and upgraded, the system automatically reloads. On boot up, the system copies the configuration file from the USB drive. Then the system reloads with the updated image and the new configuration. If there are multiple configuration files in the USB drive, the configuration files are copied in the following order (in descending priority):

- *model*.cfg for example "ICX7650.cfg,"ICX7150.cfg"
- “default.cfg”

Upgrade using manifest file in the USB

Beginning with FastIron 08.0.90, the **copy disk0 system-manifest** command can be used to copy the manifest file from USB. The images stored in the USB disk are copied to the primary or secondary partition based on the choice of partition. This image can be an application image or a Unified FastIron Image (UFI).

If you are upgrading the system to 08.0.80 or later releases, the system will upgrade the images using UFI.

If you are downgrading the system to 08.0.70 or an earlier release, only the application image is supported.

NOTE
RUCKUS does not recommend non-UFI downgrades.

copy disk0 system-manifest *file-name primary/secondary router/switch*

The parameter ***file-name*** is the name of the manifest file.

The ***primary/secondary*** parameter specifies the upgrade location. This option will download the boot image and application image for any manifest download.

The ***router/switch*** option downloads the specified images. If neither option is specified, images corresponding to the running version are downloaded. For example, if a switch build is running, switch images are downloaded from the manifest folder.

NOTE
After the USB image download, use the **unmount disk0** command before removing the disk.

After the manifest file is successfully downloaded, the manifest.txt file in the flash is retained for any future reverse manifest.

If the image is not successfully downloaded from the manifest file, the following warning message is displayed on the console.

WARNING: Possible failure on one of the member units while downloading the image. Images may not be in sync after reloading.

The user can upgrade the failed member unit at this point. If the user reloads the system, an image mismatch occurs, and the auto-copy feature upgrades the unit.

NOTE
The **all-images-primary** and **all-images-secondary** options for manifest download is deprecated beginning in release 08.0.90.

Auto-download using USB

When the system boots up, it checks for a valid manifest file, and if the manifest file is available, the system begins copying the files from the USB drive to the system flash memory. The system copies the images only through manifest file download and picks only the image listed in the manifest file. The system also copies the signature file and boot image files listed by the manifest file. It is recommended that the USB drive contain only one

manifest file set. If there are multiple manifest files in the USB drive, the system selects the first available manifest file (the order of the manifest files is not defined). The image and boot image in the USB drive must be a different version than in the system flash memory.

Image auto-copy feature

In case of an image mismatch between control bridge and port extender images, the mismatched port extender images can be upgraded using a configured TFTP server.

Beginning with 08.0.90, the correct image stored in the USB is used to upgrade and reload the mismatched port extender images.

First, we will look for the correct image in the TFTP server. If the TFTP server does not have the correct image, the image in the USB is used. The correct image stored in the USB is used for port extender. If the USB does not have the correct image, the port extender will remain in a mismatched state.

The USB status mode LED indicates the status of boot from USB and is present only for ICX 7650 and ICX 7850 devices. Refer to the platform-specific hardware installation guide for more information.

Copying UFI and Manifest Package from System Flash to USB

Beginning with FastIron release 09.0.00, you can copy UFI and manifest package from system flash to USB using CLI. The same USB can be plugged-in to another system for copying the UFI and manifest packages. This feature enables you to take backup of UFI or manifest package to a USB before performing any upgrade process.

The USB led blinks green to show that the UFI or manifest copy is in progress. The led turns to steady green once the copy is completed successfully. If the copy fails either due to flash read issue or USB access/write issue the led will blink in amber to notify the failure. During the entire operation of this UFI or manifest copy, the flash will be locked to avoid any other flash operation.

The following error message displays when there is not enough file system space available in USB.

Not enough space on the filesystem to copy the source file.

While copying the manifest package from flash to USB, the system will copy the manifest file, UFI, UFI signature and configuration file to USB. Going forward, the manifest package contains only the UFI for all ICX 7K devices.

Commands for Copying from Flash to USB

To initiate the copy of UFI from flash to USB using the CLI, enter one of the following commands:

copy flash disk0 ufi-primary <ufi image name> - Use this command to copy the primary partition's UFI to USB in the name as specified in <ufi image name>.

copy flash disk0 ufi-secondary <ufi image name> - Use this command to copy the secondary partition's UFI to USB in the name as specified in <ufi image name>.

Use the **copy flash disk0 system-manifest** command to copy the manifest package on the current running partition's UFI and UFI signature to USB.

Limitations

When one partition has legacy image (for example, 08.0.70) and another partition has UFI, copying UFI and manifest package to USB from a partition that has legacy image is not supported.

If there is a flash corruption in the system, the configurations, logs and also the UFI will be lost. In this case, copying UFI and manifest package to USB is not possible. But we can still copy the FastIron Image to USB using the existing **copy flash disk0** command, since the partition for Fastiron image is different.

OS prompt recovery procedures

NOTE
Beginning with FastIron release 09.0.00, the **no password** command is no longer supported at the uboot> prompt. Refer to "Password and Device Recovery" in the *RUCKUS FastIron Management Configuration Guide* guide for information on password recovery.

If during an upgrade procedure, the ICX device enters the OS mode and does not exit, use the **copy tftp flash** command at the OS> prompt to re-install the image.

The following example downloads the FastIron 09.0.00 UFI image from the TFTP server at the specified IP address to primary flash memory in the ICX device.

```
OS> copy tftp flash 192.168.10.89 SPR9000ufi.bin primary
```

To configure the IP address, subnet mask, and default gateway for an ICX device in OS mode, use the remote_address and remote_gateway commands and shown in the following example.

```
OS> remote_address 10.176.132.159 255.255.255.128
OS> remote_gateway 10.176.132.129
```

To copy the FastIron image from the remote TFTP server to the ICX device at the OS prompt, use the copy tftp flassh command followed by the IP address of the server, the correct image name, and the target flash location (primary or secondary) as shown in the following example.

```
OS> copy tftp flash 10.176.198.42 SPR09000ufi.bin secondary
Copying SPR09000ufi.bin from 10.176.198.42
SPR09000ufi.bin     100% |*******************************|
```

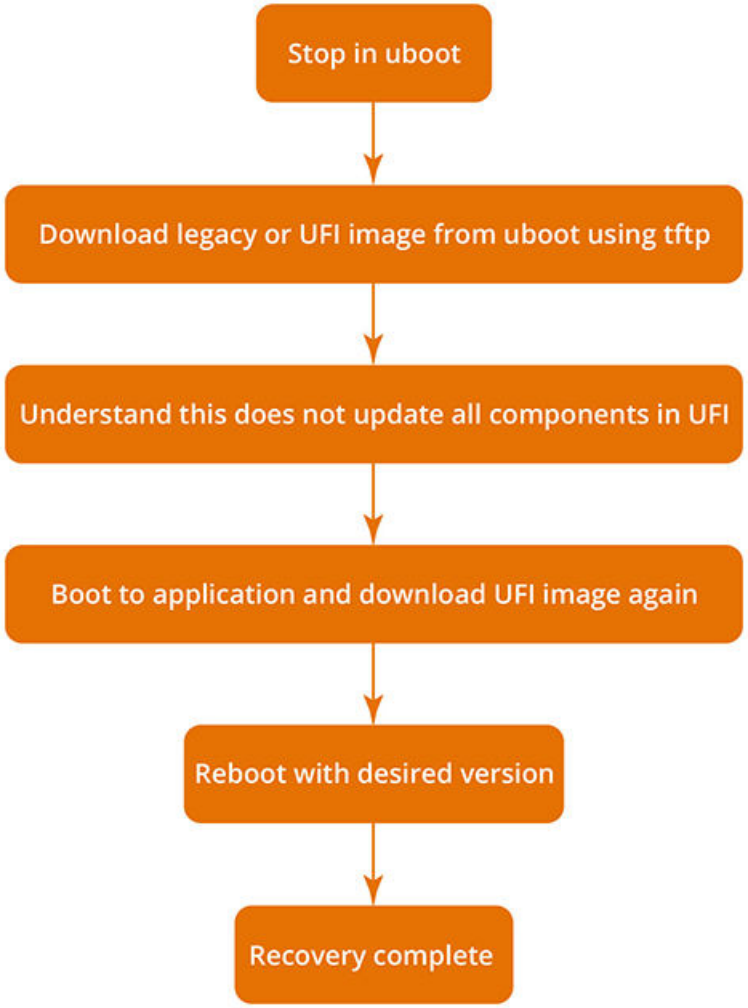
Software Recovery

If the software upgrade or downgrade fails, the device may reboot continuously as shown in the following CLI output.

```
bootdelay: ===
Booting image from Primary
Bad Magic Number
could not boot from primary, no valid image; trying to boot from secondary
Booting image from Secondary
Bad Magic Number
## Booting image at 01ffffc0 ...
Bad Magic Number
## Booting image at 01ffffc0 ...
Bad Magic Number
could not boot from secondary, no valid image; trying to boot from primary
Booting image from Primary
Bad Magic Number
## Booting image at 01ffffc0 ...
Bad Magic Number
```

Recovering Software

FIGURE 1 Recovery procedure



This section explains how to recover devices from image installation failure or deleted or corrupted flash images.

NOTE
Software recovery should be performed under the supervision of a RUCKUS support engineer.

NOTE
To stop at the uboot prompt from the console, continuously press **b** during the boot process.

1. Connect a console cable from the console port to the terminal server.
2. Connect an Ethernet cable from the management port (the port located under the console port on the device) to the TFTP server.

   The device will be in boot mode for recovery.

3. Display the existing variables from the boot prompt.

```
ICX7150-Boot> printenv
baudrate=9600
ipaddr=10.176.134.154
serverip=10.176.195.200
netmask=255.255.255.128
gatewayip=10.176.134.129
uboot=mnz10120b35.bin
image_name=SPR08095d.bin
ver=10.1.20b35T225 (Apr 29 2021 - 23:48:55 -0700)
```

   The path is to the boot image on the TFTP server.

4. Set the TFTP server that hosts a valid ICX software image using the **setenv serverip** command.

```
ICX7150-Boot> setenv serverip 10.10.10.21
```

5. Set the IP address, gateway IP address, and netmask for the device management port, and save the configuration using the **setenv ipaddr**, **setenv gatewayip**, **setenv netmask**, and **saveenv** commands.

```
ICX7150-Boot> setenv ipaddr 10.10.10.22
ICX7150-Boot> setenv gatewayip 10.10.10.1
ICX7150-Boot> setenv netmask 255.255.255.0
ICX7150-Boot> saveenv
```

   NOTE
   The IP address and the gateway IP address set for the device management port should be for the same subnet as the TFTP server NIC.

6. Enter the **printenv** command to verify the IP addresses that you configured for the device and the TFTP server.

```
ICX7150-Boot> printenv
baudrate=9600
ipaddr=10.176.134.154
serverip=10.176.195.200
netmask=255.255.255.128
gatewayip=10.176.134.129
uboot=mnz10120b35.bin
image_name=SPR08095d.bin
ver=10.1.20b35T225 (Apr 29 2021 - 23:48:55 -0700)
```

7. Test the connectivity to the TFTP server from the device using the **ping** command to ensure a working connection.

```
ICX7150-Boot> ping 10.10.10.21
ethPortNo = 0
Using egiga0 device
host 10.10.10.21 is alive
```

8. Provide the file name of the image that you want to copy from the TFTP server using the **setenv image_name** command.

```
ICX7150-Boot> setenv image_name SPR09000ufi.bin
```

9. Update the flash using the **update_primary** or **update_secondary** command as appropriate.

```
ICX7150-Boot> update_primary
```

10. Load the image from the primary or secondary flash using the **boot_primary** or **boot_secondary** command as appropriate.

```
ICX7150-Boot> boot_primary
```

Deprecated or Removed Features and Commands

For a complete list of commands deprecated in a release, refer to the release-specific *RUCKUS FastIron Command Reference* or the *RUCKUS FastIron Release Notes*. The release notes also include information about feature changes.

In-service Software Upgrade

What Is an In-service Software Upgrade?

An in-service software upgrade (ISSU) allows stack units to be upgraded with minimal interruptions to multi-unit topologies.

ISSU provides an incremental method to upgrade traditional stacks. A successful ISSU does not affect uplink or downlink connectivity in a topology with multi-unit LAGs. Only the node that is undergoing the upgrade requires a hardware reset that includes the reset of the packet processor. As a result, traffic transiting only that node is disrupted.

ISSU Limitations and Considerations

When using ISSU, consider the following capabilities and restrictions:

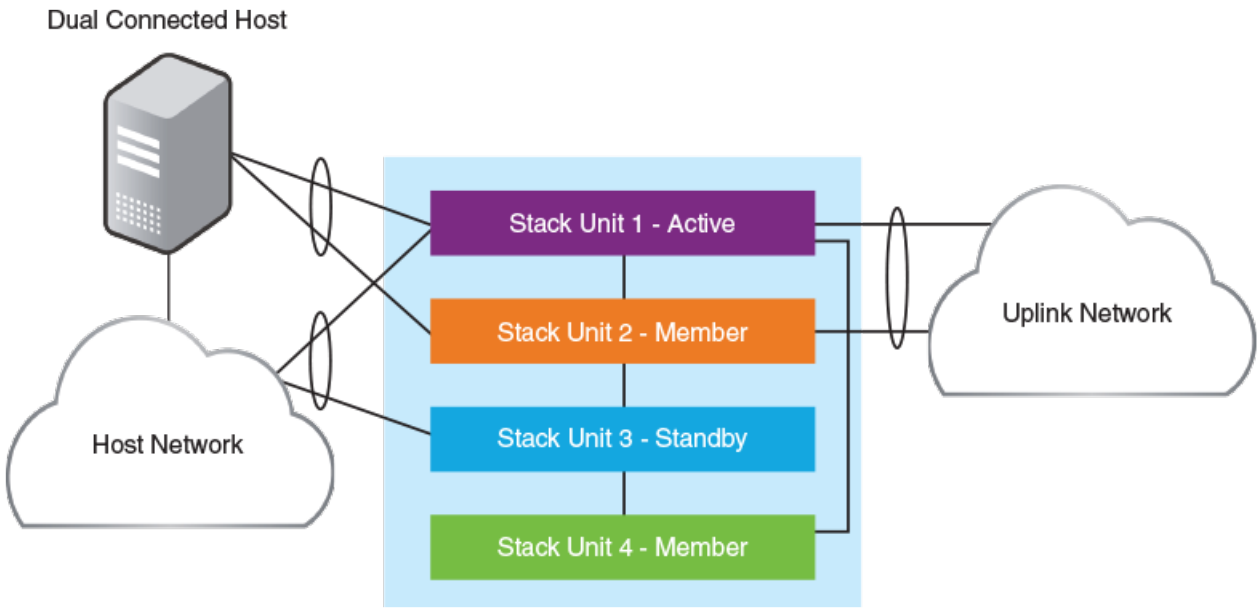
- ISSU is supported on FastIron ICX 7150, ICX 7250, ICX 7450, ICX 7550, ICX 7650, and ICX 7850 stackable hardware.
- ISSU is supported in a traditional ring stack topology.
- ISSU works for stacks of two units to the maximum supported twelve units.
- ISSU is supported for upgrades between minor releases only. For example, you can use ISSU to upgrade between FastIron 08.0.90 and FastIron 08.0.90a or between FastIron 08.0.90a and subsequent patch releases but not between FastIron 08.0.80 and FastIron 08.0.90.
- For ISSU to occur with minimal disruption, the customer network connected to the stack must have redundant uplink and downlink configurations across multiple units.
- If the secondary partition is upgraded, this partition is set as the default boot partition for the stack.
- Most CLI commands, SNMP, and web operations are blocked while ISSU is in progress.
- To make the upgrade seamless, the following administrative operations are blocked while ISSU is in progress:
  - Configuration
  - Image download to flash memory
  - Stack commands that may result in topology change or discovery
  - Initiation of another ISSU

Recommended Stack Topology for ISSU

ISSU provides an ability to upgrade traditional stacks without affecting the network.

ISSU reduces its network impact only if redundant uplink and downlink connections are available from multiple stack units. A typical topology where ISSU can be used effectively is shown in the following figure.

FIGURE 2 Recommended Stack Topology for ISSU



In the figure, redundant links are going to both the uplink network and the downlink network from different units of the stack. At any point during the upgrade, the uplink and downlink connectivity is maintained. The following software features are used to provide link redundancy:

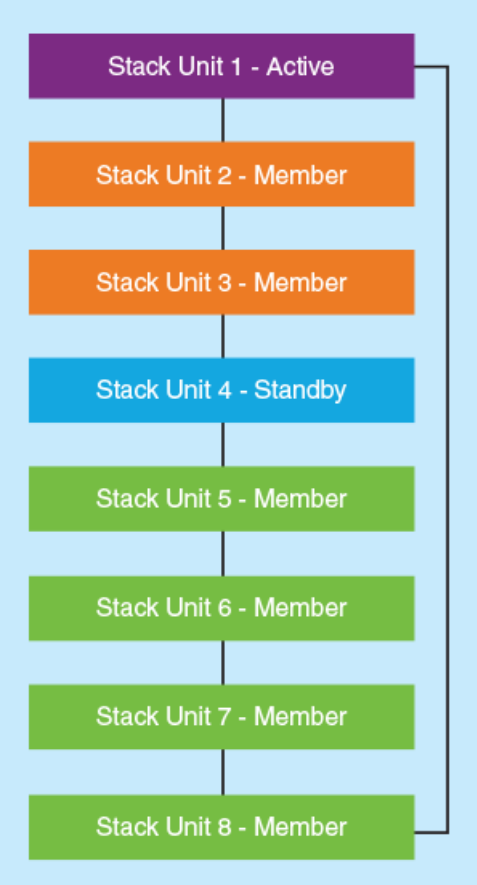
- Link aggregation (or dual connectivity to two different PEs in a chain or ring to provide PE redundancy)
- VRRP and VRRP-E
- Graceful restart for IP routing features

The node that is being upgraded goes through a hardware reset. This resets the packet processor, and traffic flowing through that specific node is disrupted.

How ISSU Works When Upgrading Stack Units

The following section describes the checks and the upgrade sequence for the typical 8-unit stack shown in the Figure 3. For a step-by-step procedure on performing an ISSU, refer to Upgrading a Stack with ISSU on page 48.

FIGURE 3 Stack Units To Be Upgraded



After you have downloaded release software as described in Initial Steps on page 13 and Upgrade Process on page 27, you can check the sequence in which stack units will be upgraded using the **show issu sequence** command. The following example displays the ISSU upgrade sequence for the stack shown in Figure 3.

```
device# show issu sequence
Stack units will be upgraded in the following order
ID Type Role
4 ICX7450-32ZP standby
3 ICX7450-32ZP member
2 ICX7450-32ZP member
5 ICX7450-32ZP member
6 ICX7450-32ZP member
7 ICX7450-32ZP member
8 ICX7450-32ZP member
1 ICX7450-32ZP active
```

All stack ISSU processes follow the same pattern. As reflected in the sample output, the stack in our example responds to the **issu** command in the following ways:

- Unit 4, the standby controller, is reloaded with the new image.
- Once the standby controller joins the stack, all member units from the standby controller to the active controller units (3 and 2 in the following example) reload the new image.
- All members from the standby controller to the active controller in the other direction (5,6,7, and 8 in the following example) reload the new image.

- Once all member units and the standby controller are reloaded with the new image, the active controller unit triggers a switchover, in which the old standby controller (4) becomes the new active controller unit, and the old active controller (unit 1) becomes the new standby controller.
- The new active controller (unit 4) reloads the old active controller (unit 1) with the new image.
- Once the old active controller (unit 1) comes up as a member unit and rejoins the stack, standby controller election occurs, and the stack becomes fully functional with the upgraded image.

  NOTE
  If the stack unit configurations have priority settings, a final switchover is done to ensure that the unit with the highest priority becomes the active controller unit.

Pre-ISSU Compatibility Checks for a Traditional Stack

After ISSU is triggered, but before ISSU processing begins, a pre-ISSU compatibility check is executed.

The compatibility check determines whether the stack is ready for an upgrade. A successful compatibility check for a stack displays the passing results shown in the following table.

TABLE 7 Pre-ISSU Checks for a Traditional Stack

Check	Passing Result
Stacking Topology is Ring	Yes
Standby Present	Yes
Standby ready for upgrade	Yes
Flash use in progress	No
Stack interactive-setup in progress	No
Stack ZTP is configured	No
ISSU in progress or aborted	No
Election pending	No
Election in progress	No
Reload pending	No
CPU utilization high	No
All units in ready state	Yes
Primary Image is upgrade compatible	Yes
Secondary Image is upgrade compatible	Yes
Startup config and Running Config Same	Yes
Boot option present in running config	No
User in Config mode	No
POE-Firmware Download is in Progress	No
System ready for issu	If this flag is present, you can proceed with ISSU. Otherwise, check the conditions flagged by three asterisks (***) and make prescribed corrections to the device before performing an ISSU.
ISSU not in progress	

Upgrading a Stack with ISSU

The following examples for copying images represent typical use. Other options such as manifest-based image copy can also be used. Refer to Initial Steps on page 13 and Upgrade Process on page 27 for more information before performing the upgrade.

Complete the following steps to upgrade a stack using ISSU.

NOTE
By default, switches are booted from the primary partition.

1. Copy the images.
   a) Back up the running image to the secondary partition.

```
device# copy flash flash secondary
```

   b) Copy the new image from its server location to the primary partition.

```
device# copy tftp flash 10.10.10.10 SWR08090aufi.bin primary
```

   The IP address in the example is for the TFTP server. The address can be an IPv4 or IPv6 address. The .bin file is the name of the image file.
2. Check the sequence of the upgrade.

```
device# show issu sequence
Stack units will be upgraded in the following order
ID Type Role
1 ICX7450-32ZP standby
3 ICX7450-32ZP member
4 ICX7450-32ZP active
```

   The example shows the sequence for a three-unit stack.

3. Initiate the upgrade.

   Use the **issu primary** command, preferably with an error recovery option, if you downloaded the image to the primary partition of the flash.

   Or use the **issu secondary** command, preferably with an error recovery option, if you downloaded the image to the secondary partition.

   NOTE
   RUCKUS recommends using an error recovery option when upgrading.

   NOTE
   The issu command option **on-error reload-primary** shown in the following example specifies an automatic reload from the primary partition if there is an upgrade error. You can also specify the option **on-error reload-secondary** to reload from the secondary partition to bring the stack back up with the original image.

- Initiating the upgrade with error recovery.

```
device# issu primary on-error reload-primary
Stacking Topology is Ring               Yes
Standby Present                         Yes
Standby ready for upgrade               Yes
Flash use in progress                   No
Stack interactive-setup in progress     No
Stack ZTP is configured                 No
ISSU in progress or aborted             No
Election pending                        No
Election in progress                    No
Reload pending                          No
CPU utilization high                    No
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
Proceed with upgrade? (enter 'y' or 'n'):
```

- Initiating the upgrade without error recovery (not recommended)

```
device# issu secondary
Stacking Topology is Ring               Yes
Standby Present                         Yes
Standby ready for upgrade               Yes
Flash use in progress                   No
Stack interactive-setup in progress     No
Stack ZTP is configured                 No
ISSU in progress or aborted             No
Election pending                        No
Election in progress                    No
Reload pending                          No
CPU utilization high                    No
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
Proceed with upgrade? (enter 'y' or 'n'):
```

If an error occurs when the upgrade was initiated without error recovery, the error condition is marked by three asterisks.

```
device# issu primary
Stacking Topology is Ring               Yes
Standby Present                         No   ***
Standby ready for upgrade               No   ***
```

```
Flash use in progress                   No
Stack interactive-setup in progress     No
Stack ZTP is configured                 No
ISSU in progress or aborted             No
Election pending                        No
Election in progress                    No
Reload pending                          No
CPU utilization high                    No
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
System not ready for issu. Check error condition highlighted by "***" and rectify.
ISSU not in progress
```

4. Enter **y** when prompted to start the upgrade, or **n** to stop the process.

5. Wait for the upgrade to complete, and check the status. (You may check the status at any time.)

   The following **show issu status** command output indicates the successful completion of an ISSU upgrade.

```
device# show issu status
Last upgrade time 00:02:19.367 GMT+00 Tue Mar 20 2019
The older image before-ISSU SPR08090.bin
Stacking Topology is Ring               Yes
Standby Present                         Yes
Standby ready for upgrade               Yes
Flash use in progress                   No
Stack interactive-setup in progress     No
Stack ZTP is configured                 No
ISSU in progress or aborted             No
Election pending                        No
Election in progress                    No
Reload pending                          No
CPU utilization high                    No
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
System ready for issu
ISSU not in progress
```

   The following example shows a status display for an upgrade that is in progress.

```
device# show issu status
ISSU Status: In Progress
Upgrade State: UNIT JOIN
Upgrade Option: issu primary
ID   Type          Role      State
1    ICX7450-32ZP  member    UPGRADING
3    ICX7450-32ZP  member    UPGRADE PENDING
4    ICX7450-32ZP  active    UPGRADE PENDING
```

   If the upgrade has not been initiated, the **show issu status** command displays information about whether the system is ready for the upgrade.

   The following example shows a status display for an aborted upgrade.

```
device# show issu status
ISSU Status: Aborted
Upgrade State: UPGRADE ABORT
Upgrade Option: issu primary
Reason for Abort: UNABLE TO UPGRADE
ID   Type          Role      State
1    ICX7450-32ZP  member    UPGRADE ABORT
3    ICX7450-32ZP  standby   UPGRADE PENDING
4    ICX7450-32ZP  active    UPGRADE PENDING
```

   The following example shows an unsuccessful ISSU that was aborted due to a hot swap error.

```
device# show issu status
 Abort info before recovery upgrade:
         Reason for abort                HOTSWAP ERROR
         Hotswap error with Unit 1
 Topology is Ring                        Yes
 Standby Present                         Yes
 Standby ready for upgrade               Yes
 Flash use in progress                   No
 Stack interactive-setup in progress     No
 ISSU in progress or aborted             No
 Election pending                        No
 Election in progress                    No
 Reload pending                          No
 CPU utilization high                    No
```

```
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
System ready for issu
ISSU not in progress
```

If the upgrade is aborted manually or if ISSU detects an abort condition (when the **issu** command is used without the **on-error** option), the stack is left as it is, and a manual recovery is required.

Summary ISSU Command Sequence for Upgrading a Stack

```
device# copy flash flash secondary
device# copy tftp flash 10.10.10.10 SWR0809a0ufi.bin primary
device# show issu sequence
device# issu primary on-error reload-primary
device# show issu status
```

ISSU Errors

There are several sources of errors that may be encountered during an ISSU, and there are two means of error recovery.

TABLE 8 Common Errors

Check	Passing Result
Hot-swap timeout	Unit hot-swap does not complete within the expected time.
Version synchronization timeout	Version information synchronization does not complete within the expected time.
Standby assignment timeout	After upgrading the current standby unit, the standby assignment does not occur within the expected time.
Standby assignment error	After upgrading the current standby unit, the expected unit was not elected as the new standby unit.
Image/boot source mismatch	After a unit upgrade, the image version and boot source did not match the expected version or boot source.
Unit fails to rejoin	The unit fails to rejoin the stack within the specified time after an upgrade.
Unit delete	The unit is detached from the stack while the ISSU is in progress.
Ping fail	A unit fails to respond to keepalive messages.

TABLE 9 Crash and Manual Abort Errors

Error Message	Description
Unit crash	If the **issu** command **on-error** option is specified, the unit that crashes is reloaded from the partition specified in the command. The active controller detects this condition as a unit delete and reloads all the existing stack members from the partition specified in the **issu** command **on-error** option.

TABLE 9 Crash and Manual Abort Errors (continued)

Error Message	Description
Active reload/crash	If the active controller reloads unexpectedly, or crashes while the ISSU is in progress, the stack units detect the loss of the active controller and abort the ISSU. If the **issu** command **on-error** option is specified, all units that were part of the stack at the time of the active controller crash are reloaded from the partition specified in the command. Any units that were being upgraded at the time of the active controller failover reload from the target partition given in the **issu** command. Once all units have booted and an active controller has been elected, if some units have a running image different from the active controller image, an **image auto-copy** is executed, and units are reloaded to ensure they are all running the same image.
Manual abort	If ISSU is aborted through the **issu abort** command, ISSU is stopped, and the stack is left in the current state for manual recovery. This behavior occurs whether ISSU is started with or without the **issu** command **on-error** option.

Error Recovery

There are two means for error recovery, one manual and one automatic:

- When ISSU is started with the **issu primary** or **issu secondary** command, the following results apply:
  - If an error occurs, the upgrade is aborted, and the stack is left for manual recovery. In this condition, it is likely that the running images on the stack units are different. After abort, **image auto-copy** is not executed.
  - Units continue with their current running image until the system is reloaded. As a result, a reload of the entire stack is required to bring it back to a functional state.
  - To ensure system stability, the stack is left in the aborted state. You must reload the system manually. If any of the stack units are reloaded individually, they cannot move to the Ready state. To execute a manual recovery, refer to Manual Error Recovery on page 54.
- The following points apply when ISSU is started with an **issu primary** or an **issu secondary** command that includes an **on-error reload primary** or an **on-error reload-secondary** option:
  - If an error occurs, the upgrade is aborted.
  - All the units in the stack are automatically reloaded to the partition specified by the **issu** command **on-error** option.
  - After the system reload, any units that were unreachable at the time of the ISSU abort may have an image that is different from the other units. When these units rejoin the stack, an **image auto-copy** is executed for any units with a mismatched image, and they are reloaded after the auto-copy completes.

Manual Error Recovery

Complete the following steps to manually recover from an ISSU error.

If an error is detected during the upgrade, ISSU is aborted. In this case, the recommended procedure is to reload the stack to the old or new image from the primary or secondary partition, and then use the **boot system flash** command to reload the stack.

1. Reload to the primary partition.

```
device# boot system flash primary
```

2. Reload to the secondary partition.

```
device# boot system flash secondary
```

COMMSCOPE®
RUCKUS®

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