Ruckus FastIron Software Upgrade Guide, 08.0.70

Supporting FastIron Software Release 08.0.70

Part Number: 53-1005298-01
Publication Date: 21 December 2017

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ARRIS and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. ARRIS and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL ARRIS or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, ICX, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

Preface

Document Conventions

The following tables list the text and notice 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 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.

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.

Convention	Description
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.

Document Feedback

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

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

When contacting us, please include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)
- For example:
  - Ruckus Small Cell Alarms Guide SC Release 1.3
  - Part number: 800-71306-001
  - Page 88

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

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

Online Training Resources

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

Contacting Ruckus Customer Services and Support

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

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

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. Request 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, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.

Self-Service Resources

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

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

About this Document

What's new in this document

TABLE 2 Summary of enhancements in FastIron release 8.0.70

Feature	Description	Location
SPX In-service Software Upgrade (ISSU)	Campus Fabric (SPX) networks can be upgraded using ISSU.	Refer to In-service software upgrade on page 38 for additional information.
Boot from USB	Software upgrade can be done through manifest file download using USB drive.	Refer to Boot from USB on page 34.
System backup to USB	Allows you to copy files from the system flash memory to the connected USB drive.	Refer to System backup to USB on page 35.

Supported hardware

This guide supports the following Ruckus products:

- Ruckus ICX 7750 Series
- Ruckus ICX 7650 Series
- Ruckus ICX 7450 Series
- Ruckus ICX 7250 Series
- Ruckus ICX 7150 Series

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

Upgrade and Downgrade Considerations

Upgrading to or downgrading from FastIron 8.0.xx

NOTE
You must upgrade both the boot code and flash image that supports this release before rebooting. Refer to "Software image files for Release 8.0.xx" in the release notes for detailed information.

Static routing and IPv6 features enabled in base license

FastIron release 8.0.40 introduced IPv6 static routing as part of the base license for ICX devices. This feature was previously available only under the premium license. If you downgrade to an earlier release that is covered by a premium license, there is no impact. If the earlier release is not covered by a premium license, any IPv6 static routing configuration is lost. Refer to the *Brocade FastIron Software Licensing Guide* for more information on licensing changes.

General considerations

Upgrade considerations

- If upgrading from either FastIron release 8.0.40 or 8.0.40a to FastIron 8.0.50, after the upgrade you must add `/guest` to the address of the captive portal login page, so that the address `.../test.php` reads `.../guest/test.php`.
- There are two ways to upgrade the software. You can perform a manual (step-by-step) upgrade or upgrade through a manifest file. Refer to the chapter Software Upgrade and Downgrade on page 19.
- MACsec in FastIron releases 8.0.20a onward, is not compatible with previous versions of the MACsec feature due to changes in CLI functionality. An upgrade is required.
- If configured, syslogs do not persist across reloads.

ATTENTION
There is a change in the default route configuration between the FastIron 7.x and FastIron 8.x releases. In the FastIron 8.x releases, the default route next hop cannot be configured as an GRE tunnel, VE, or physical port interface, which was supported in 7.x releases.
Before you upgrade from FastIron 7.x to FastIron 8.x, you must change the default GRE tunnel number to the GRE tunnel IP address. Otherwise, connectivity is lost after the upgrade. For example on a device running FastIron 7.4 the following output is seen the In the running configuration:

```
device# show running-config | include ip route
ip route 10.10.10.10 0.0.0.0 tunnel 1
```

To change the GRE IP route configuration:

```
device(config)# ip route 10.10.10.10 0.0.0.0 10.11.11.11
device(config)# exit
device# show running-config | include ip route
ip route 10.10.10.10 0.0.0.0 10.11.11.11
```

Where 10.11.11.11 is the IP address at the other end of the GRE tunnel.

Downgrade considerations

- After a downgrade from release 8.0.50, the uplink switch feature is not supported.
- Release 8.0.50 allows ICX 7250 as a Port Extender. As such, ICX 7750 allows reserved configuration of ICX 7750, ICX 7450 and ICX 7250. When a CB containing ICX 7250 provisional configuration downgrades to Release 8.0.40, all ICX 7250 configuration is rejected.
- When downgrading to a version earlier than FastIron 8.0.10, software-based licensing is not supported.
- SSHv2 RSA host key format may differ among FastIron software versions.
- If you downgrade to FastIron 8.0.40 and if the saved configuration has options enabled (e.g., IPsec, IKEv2) that do not exist in the earlier release, then an error message is displayed while the system is parsing the configuration. To avoid this type of error message, delete the enabled options then save the configuration before you downgrade to FastIron 8.0.40.
- If you downgrade to FastIron 8.0.40, before the downgrade you must enable LLDP at a global level by executing an **ldap run** command followed by a **write memory** command. Otherwise, the 802.1br (Bridge Port Extension) setup might fail to form and a warning is displayed in the output of the **show spx** command: `Warning! has "spx-cb-enable" config but no "lldp run"`.
- Upon a downgrade, you may observe the following with policy based routing (PBR) over VRF:
  - If PBR is enabled on the VRF aware interface, it is removed on downgrade.
  - You may receive an error when executing the **next hop** command with VRF if you boot up using the `running-config` file.

    NOTE
    For more information about PBR over VRF, see the *Brocade FastIron Security Configuration Guide*.
- The ICX 7250 and 7450 must run 8.0.50 image to be discovered by the zero touch or SPX interactive-setup feature. By default, DHCP client is enabled on these products. Therefore, customers can configure a DHCP and TFTP server to push new images to ICX 7250 and ICX 7450 when they link to networks or a SPX system.
- During the downgrade from a version where a sequence number is supported to lower version where it is not supported, the global suppress ACL sequence command - **supress acl-sequence** must be executed before saving the configuration.

  If the **suppress acl-sequence** command is not enabled before downgrade, The ACL configurations created with sequence parameter on 8.0.50 release persist in the earlier release, and result in an error.

- If the PVLAN Dual Mode Support feature is enabled, if you downgraded to FastIron 08.0.40 or older releases, errors are thrown during parsing time as this configuration is not supported before the FastIron 08.0.50 release.
- All specific Route-only feature configurations are lost on downgrade.
- If Layer 2 Mode Querier Address feature is enabled, when you downgrade to an older release, the system throws a command not recognized error.

Deprecated or removed features and commands

- SNTP is no longer supported. NTPv4 replaces SNTP.
- The Port Speed Down-Shift feature is deprecated in FastIron 08.0.xx.
- The **stack persistent-mac-timer** command is deprecated in FastIron 08.0.20.
- The **link-config gig copper autoneg-control down-shift ethernet** command is deprecated.
- The **show cpu-utilization** command replaces the **show process cpu** command.

Flash memory capacity

All FastIron devices can hold two Layer 2 or Layer 3 images (for example, SWS08050.bin for Layer 2 and SWR08050.bin for full Layer 3).

Considerations for devices in stack configurations

Upgrade considerations

- Hitless stacking is enabled by default for FastIron 8.0.20 and later releases. In previous releases, **hitless-failover enable** must be configured. Upgrade behavior is as follows:
  – Upgrading to FastIron release 8.0.30 or 8.0.40 from a system running release 8.0.10 configured with **hitless-failover enable** - You must manually configure **hitless-failover enable.**
  – Upgrading to FastIron release 8.0.20 from an earlier version with **hitless-failover enable** configured - Hitless failover is retained as the default.
  – Upgrading to FastIron release 8.0.20 or later on a system running an earlier release that does not have **hitless-failover enable** configured - The previous configuration is retained; hitless stacking failover is not enabled.
  – Installing a FastIron release 8.0.20 or later image on a new system with no previous configuration. - Configured with **hitless-failover enable** is the default.
- Units in a stack must run the same IPC version to communicate. After an upgrade, verify that the same image is downloaded to every unit in the stack before reloading the entire stack. To verify the images, enter the **show flash** command at any level of the CLI. A stack cannot be built and does not operate if one or more units have different software images.
- A stack cannot form if the software images are of different major versions. A stack member is not operational if it runs a different minor version from other stack members. However, the active controller can download an image and reset a non-operational unit that has a minor version number different from the active controller.
- A stack cannot form if the software images are of different major versions. A stack member is not operational if it runs a different minor version than other stack members; however, the active controller can download an image and reset a non-operational unit that has a minor version number different from the active controller.
- The Layer 3 configuration on your device becomes part of the default VRF after upgrade. If no configurations are done, all interfaces are part of the default VRF.

Upgrade considerations for devices with flexible authentication

The following behavior associated with flexible authentication should be taken into consideration when you upgrade or downgrade FastIron.

The **authentication vlan-mode** command, introduced in FastIron 8.0.30b, affects upgrades and downgrades as summarized in the following tables.

TABLE 3 Flexible authentication upgrade results

FastIron upgrade scenario	vlan-mode	Comments
8.0.10 to 8.0.20	Multiple untagged	Port can be part of multiple VLANs.
8.0.10 to 8.0.30b and later releases	Single untagged	After upgrade, the default behavior is single untagged. If required, this default behavior can be changed to multiple untagged using the new CLI.
8.0.20 to 8.0.30b and later releases	Single untagged. There are no changes to the configuration.	After upgrade, the default behavior is single untagged. If required, this default behavior can be changed to multiple untagged.

TABLE 4 Flexible authentication downgrade results

FastIron downgrade scenario	vlan-mode	Comments
8.0.30b and later releases to 8.0.20	Multiple untagged	The new **authentication vlan-mode** command configuration is lost.
8.0.30b and later releases to 8.0.10x	Single untagged	All flexible authentication configuration is lost. You must reconfigure as per CLI syntax in FastIron 8.0.10x.
8.0.20 to 8.0.10x	Single untagged	All flexible authentication configuration is lost. You must reconfigure as per CLI syntax in FastIron 8.0.10x.

FastIron 8.0.30b introduced support for the **authentication max-sessions** command on ICX 7250, ICX 7450, and ICX 7750 devices. Consequently, when you upgrade to or downgrade from FastIron 8.0.40, CLI behavior changes. The following tables summarize changes for different FastIron devices.

TABLE 5 Upgrade behavior for the authentication max-sessions command

FastIron upgrade scenario	Behavior	Comment
8.0.10 to 8.0.20	Maximum = 32 users	For ICX 7450 and ICX 7750 devices, the default is 32 and cannot be changed.
8.0.10 to 8.0.30b and later releases	Default = 2 users	Can be configured to a maximum of 256 or 1024, depending on the type of device.
8.0.20 to 8.0.30b and later releases	Default = 2 users	Can be configured to a maximum of 256 or 1024, depending on the type of device.

TABLE 6 Downgrade behavior for the authentication max-sessions command

FastIron downgrade scenario	Behavior	Comment
8.0.30b and later releases to 8.0.20x	Maximum = 32 users	Configuration is lost on downgrade when the configured max-sessions value is greater than 32.
8.0.30b and later releases to 8.0.10x	Maximum = 250 users	Configuration lost on downgrade.
8.0.20 to 8.0.10x	Maximum = 250 users	Configuration lost on downgrade.

Refer to the *Brocade FastIron Security Configuration Guide* and the following sections for more information on flexible authentication.

Dot1x authentication and MAC authentication configured on default VLAN on page 15

Dot1x authentication and MAC authentication configured on a VLAN other than the default VLAN on page 16

Dot1x authentication and MAC authentication configured on a voice VLAN on page 17

Dot1x authentication and MAC authentication configured on default VLAN

Beginning with the FastIron 8.0.20 release, after you upgrade, global configuration for both dot1x authentication and MAC authentication move under the authentication section. The first unused VLAN becomes the authentication default VLAN (the auth-default-vlan), shown as VLAN 2 in the following example. Interface level configuration for dot1x authentication and MAC authentication conform to any new CLI changes that are part of the upgrade.

In the example shown below, before an upgrade, the configured ports are part of the default VLAN. Authentication with dot1x is enabled on port 2/1/24 and MAC authentication is enabled on port 2/1/23 both globally and at the interface level. After upgrade, since port 2/1/23 and port 2/1/24 are part of the default VLAN, they become part of the authentication default VLAN (auth-default-vlan) identified as VLAN 2.

```
vlan 1 name DEFAULT-VLAN by port  >> 2/1/24 and 2/1/23 ports are part of default vlan
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9
 untagged ethe 1/1/18
!
vlan 200 by port
untagged ethe 1/1/15
!
vlan 201 by port
!
dot1x-enable  >> global configuration
enable ethe 2/1/24
!
mac-authentication enable  >> global configuration
mac-authentication auth-passwd-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24  >> interface level
dot1x port-control auto
!
interface ethernet 2/1/23  >> interface level
mac-authentication enable
mac-authentication max-accepted-session 32
```

The following example shows the configuration after the upgrade.

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9
 untagged ethe 1/1/18
!
vlan 200 by port
untagged ethe 1/1/15
!
vlan 201 by port
!
authentication  >> dot1x and mac-auth global commands appear
                   under authentication command
auth-default-vlan 2
dot1x enable
dot1x enable ethe 2/1/24
mac-authentication enable
```

```
mac-authentication enable ethe 2/1/23
 mac-authentication password-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/23
authentication max-sessions 32
!
interface ethernet 2/1/24
dot1x port-control auto
!
```

Dot1x authentication and MAC authentication configured on a VLAN other than the default VLAN

Beginning with the FastIron 8.0.20 release, after you upgrade, global configuration for both dot1x authentication and MAC authentication move under the authentication section, and the first unused VLAN becomes authentication default VLAN (the auth-default-vlan), VLAN 2 in the following example.

In the example below, before upgrade, with dot1x authentication enabled globally on port 2/1/24 and MAC authentication enabled globally on port 2/1/23, the configured ports are part of VLANs 600 and 601. After upgrade, VLAN 600 becomes the auth-default-vlan for prot 2/1/24, and 601 becomes the auth-default-vlan for port 2/1/23.

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9
 untagged ethe 1/1/18
!
vlan 200 by port
untagged ethe 1/1/15
!
vlan 201 by port
!
vlan 600 by port
 untagged ethe 2/1/24
!
vlan 601 by port
untagged ethe 2/1/23
!
dot1x-enable  >> global configuration
enable ethe 2/1/24
!
mac-authentication enable  >> global configuration
mac-authentication auth-passwd-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24  >> interface level
dot1x port-control auto
!
interface ethernet 2/1/23  >> interface level
mac-authentication enable
mac-authentication max-accepted-session 32
```

The following example shows the configuration after the upgrade.

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9
 untagged ethe 1/1/18
```

```
!
vlan 200 by port
untagged ethe 1/1/15
!
vlan 201 by port
!
vlan 600 by port  >> 2/1/24 should be removed
!
vlan 601 by port >> 2/1/23 should be removed
!
authentication
auth-default-vlan 2
dot1x enable
dot1x enable ethe 2/1/24
mac-authentication enable
mac-authentication enable ethe 2/1/23
 mac-authentication password-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24
authentication auth-default-vlan 600
dot1x port-control auto
!
interface ethernet 2/1/23
authentication auth-default-vlan 601
authentication max-sessions 32
!
```

Dot1x authentication and MAC authentication configured on a voice VLAN

Beginning with the FastIron 8.0.20 release, after you upgrade, global configuration for both dot1x authentication and MAC authentication moves under the authentication section, and the first unused VLAN moves to the authentication default VLAN (the auth-default-vlan) section, identified as VLAN 2 in the following example. The dual-mode sections are replaced by the auth-default-vlan at the interface level. The voice-vlan section remains the same.

In the example below, before an upgrade, dot1x authentication is enabled globally on port 2/1/24 and MAC authentication is enabled globally on port 2/1/23. The tagged ports are part of VLANs 100 and 200 respectively. Both of these tagged ports are part of voice-vlan VLAN 1000. After an upgrade, VLAN 100 becomes the auth-default-vlan for port 2/1/24, and VLAN 200 becomes the auth-default-vlan for port 2/1/23. The voice-vlan section is retained.

```
vlan 1 name DEFAULT-VLAN by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9 ethe 2/1/24
 untagged ethe 1/1/18
!
vlan 200 by port
tagged ethe 2/1/23
 untagged ethe 1/1/15
!
vlan 1000 by port
tagged ethe 2/1/23 to 2/1/24
!
dot1x-enable  >> global configuration
enable ethe 2/1/24
!
mac-authentication enable  >> global configuration
mac-authentication auth-passwd-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24  >> interface level
dot1x port-control auto
```

```
dual-mode  100
voice-vlan 1000
!
interface ethernet 2/1/23  >> interface level
mac-authentication enable
mac-authentication max-accepted-session 32
dual-mode  200
voice-vlan 1000
```

The following example shows the configuration after the upgrade.

```
switch# show running-config vlan
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 3 by port
tagged ethe 1/1/5
!
vlan 100 by port
tagged ethe 1/1/9   >> 2/1/24 should be removed
untagged ethe 1/1/18
!
vlan 200 by port  >> 2/1/23 should be removed
untagged ethe 1/1/15
!
vlan 1000 by port
tagged ethe 2/1/23 to 2/1/24
!
authentication
auth-default-vlan 2
dot1x enable
dot1x enable ethe 2/1/24
mac-authentication enable
mac-authentication enable ethe 2/1/23
 mac-authentication password-format xxxx.xxxx.xxxx
!
interface ethernet 2/1/24
authentication auth-default-vlan 100
dot1x port-control auto
voice-vlan 1000
!
interface ethernet 2/1/23
authentication auth-default-vlan 200
authentication max-sessions 32
voice-vlan 1000
!
```

Software Upgrade and Downgrade

Software upgrade overview

There are two ways you can perform an upgrade, either through a manual step-by-step process or through a manifest file.

Support is available for upgrades starting at release 8.0.0.

1. For any upgrade, follow the instructions in Initial steps on page 19 to determine the current software versions, license requirements, and instructions on where to download the software.

   If configured, syslogs do not persist across reloads.

2. Upgrade the software.

   - For a step-by-step upgrade go to the section Upgrade process on page 22 then finish by referring to Loading images on the device on page 23.
   - For a manifest file upgrade go to the section Software upgrade using a manifest file on page 31.

   Upgrade both the boot code and flash image before a reload command is executed.

3. If the device is running in FIPS mode follow these steps:

   a) Signature verify the boot image that is copied to the system.

      If signature verification fails, copy a matching boot image signature file.

   b) Copy the signature file before the upgrade.

   c) After the signature file has been copied, copy the boot image.

   d) After the boot image binary has been copied, perform a signature verification.

      The data is saved to the bootrom only when there has been a successful verification.

Initial steps

- You must upgrade to the boot code that supports this release. Refer to "Software image files for Release 8.0.xx" in the release notes for detailed information.
- The output shows an upgrade done from an 8.0.30 image to 8.0.40.
- In this section, some of the output is truncated. Detailed output is shown in the following section.

Perform the following steps before an upgrade or downgrade.

1. Determine the current boot image version using the **show flash** command.

```
device# show flash
Stack unit 1:
  Compressed Pri Code size = 24108665, Version:08.0.40qT213 (SPR08040q074.bin)
  Compressed Sec Code size = 24108665, Version:08.0.40qT213 (SPR08040q074.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.06T215 (spz10106b002)
  Code Flash Free Space = 1768706048
device#
```

2. Determine the current flash image version using the **show version** command.

```
device# show version
  Copyright (c) 1996-2015 Brocade Communications Systems, Inc. All rights reserved.
    UNIT 1: compiled on May 19 2015 at 20:07:00 labeled as SPS08040b074
      (28893380 bytes) from Primary SPS08030.bin
        SW: Version 08.0.40b074T211
      Compressed Boot-Monitor Image size = 786944, Version:10.1.06T215 (spz10106b002)
  HW: Stackable ICX7450-24
...
<output is truncated to show relevant sections only>
```

3. Determine the current license installed using the **show version** command.

```
device# show version
...
License: BASE_SOFT_PACKAGE   (LID: eavIIJLmFIK)
      P-ASIC  0: type B548, rev 01  Chip BCM56548_A0
...
<output is truncated to show relevant sections only>
```

4. Generate a new license, if required, from the Software License page on Brocade.com. 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. For more information on licenses, refer to the *Brocade FastIron Software Licensing Guide*.
5. Download the required software images from the Downloads page on the MyBrocade website. For the list of software image files available for FastIron 08.0.xx, refer to the release notes.

For more information, see the sections:

Determining the flash image version on page 20

Determining the flash and boot image versions on page 21

Determining the current licenses installed on page 22.

Determining the flash image version

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

```
device# show version
Copyright (c) 1996-2015 Brocade Communications Systems, Inc. All rights reserved.
    UNIT 1: compiled on May 19 2015 at 20:07:00 labeled as SPS08040b074
      (28893380 bytes) from Primary SPS08040b074.bin
        SW: Version 08.0.40b074T211
      Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215 (spz10105)
  HW: Stackable ICX7450-24
  Internal USB: Serial #: 9900614090900038
      Vendor: ATP Electronics, Total size = 1919 MB
==========================================================================
UNIT 1: SL 1: ICX7450-24 24-port Management Module
      Serial  #:CYT3346K035
      License: BASE_SOFT_PACKAGE   (LID: eavIIJLmFIK)
      P-ASIC  0: type B548, rev 01  Chip BCM56548_A0
==========================================================================
UNIT 1: SL 2: ICX7400-4X10GF 4-port 40G Module
      Serial  #:CYV3346K07G
==========================================================================
UNIT 1: SL 3: ICX7400-1X40GQ 1-port 40G Module
      Serial  #:CYX3346K06F
==========================================================================
UNIT 1: SL 4: ICX7400-1X40GQ 1-port 40G Module
      Serial  #:CYX3346K00A
==========================================================================
 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 12 hour(s) 20 minute(s) 45 second(s)
The system : started=cold start
```

In this example:

- In the second line of the first section:

  "UNIT 1: compiled on May 19 2015 at 20:07:00 labeled as SPS08040b074"

  "SPS08040b074" is the flash code image label. This is the image type and version and is especially useful if you change the image file name.

- In the third line of the first section:

  "(28893380 bytes) from Primary SPS08040b074.bin "

  "SPS08040b074.bin" is the loaded flash code image file name.

- In the fifth line of the first section:

  " Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215 (spz10105) "

  "10.1.05T215" is the flash code version number.

- In the third line of the second section:

  "License: BASE_SOFT_PACKAGE (LID: eavlIJLmFIK)" is the license currently installed on the device.

Determining the flash and boot image versions

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

```
device# show flash
Stack unit 1:
  Compressed Pri Code size = 28893380, Version:08.0.40T211 (SPS08040b074.bin)
  Compressed Sec Code size = 28893380, Version:08.0.40T211 (SPS08040b074.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215
  Code Flash Free Space = 1776869376
device#
```

In the previous example:

- "Compressed Pri Code size" is the flash code version installed on the primary flash area.
- "Compressed Sec Code size" is the flash code version installed in the secondary flash area.
- "Compressed Boot-Monitor Image size" is the boot code version installed in flash memory.

  NOTE
  File names vary for different releases.

Determining the current licenses installed

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

```
device# show version
Copyright (c) 1996-2015 Brocade Communications Systems, Inc. All rights reserved.
    UNIT 1: compiled on May 19 2015 at 20:07:00 labeled as SPS08040b074
      (28893380 bytes) from Primary SPS08040b074.bin
        SW: Version 08.0.40b074T211
      Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215 (spz10105)
  HW: Stackable ICX7450-24
  Internal USB: Serial #: 9900614090900038
      Vendor: ATP Electronics, Total size = 1919 MB
==========================================================================
UNIT 1: SL 1: ICX7450-24 24-port Management Module
      Serial  #:CYT3346K035
      License: BASE_SOFT_PACKAGE   (LID: eavIIJLmFIK)
      P-ASIC  0: type B548, rev 01  Chip BCM56548_A0
==========================================================================
```

In this example, the second section shows that a base software package license is installed, with a license ID (LID) of eavIIJLmFIK.

What to do next

1. If required, generate a new license from the Software License page on Brocade.com. For instructions on how to generate a license, refer to the *Brocade FastIron Software Licensing Guide*.
2. Download the software from the Downloads page on the MyBrocade website to a TFTP server.
3. Perform the upgrade:
    - If you are conducting a manual (step-by-step) upgrade, go to the section Upgrade process on page 22.
    - If you are conducting a manifest file upgrade, go to the section Software upgrade using a manifest file on page 31.

Upgrade process

This release introduces several new features and enhancements across all FastIron products. Before upgrading the software on the device, refer to Upgrade and Downgrade Considerations on page 11.

> NOTE
> If you are upgrading from FastIron 8.0.10 or later, you can upgrade using a manifest file. It provides a simplified upgrade mechanism, especially for units in a stack. For details, refer to Software upgrade using a manifest file on page 31.

Software upgrade

To upgrade software on ICX 7250, ICX 7450, and ICX 7750 devices, follow the high-level steps listed below.

1. Load the boot code and flash code. For detailed steps, refer to Loading images on the device on page 23.
2. Enter the **write memory** command to back up the existing startup configuration and to save the running configuration as the startup configuration. The existing startup configuration file, startup-config.txt, is automatically copied and synched to the standby unit.

Loading images on the device

Any software upgrade or downgrade requires you to copy the downloaded images onto the device and load the new image on the device. You must load the boot code and flash code on the device.

Upgrade and downgrade software images

Software images for all Ruckus devices can be uploaded and downloaded between flash modules on the devices and a TFTP server on the network.

Ruckus 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.

You can use TFTP to copy an update image from a TFTP server onto a flash module. You can also use the Secure Copy Protocol (SCP) to copy images to and from a host. When you want to back up the current configuration and images for a device, you can copy the images and configuration files from a flash module to a TFTP server.

> NOTE
> Ruckus devices are TFTP clients, not TFTP servers. You must perform a TFTP transaction from the Ruckus device.

Loading the boot code

You can load the boot code using either TFTP or SCP as described in the following sections:

Loading the boot code using TFTP on page 23

Loading the boot code using SCP on page 24

Loading the flash code

You can load the flash code using either TFTP or SCP as described in the following sections:

Loading the flash code using TFTP on page 24

Loading the flash code using SCP on page 26

> NOTE
> It is strongly recommended that you use SCP for reliable and secure loading of flash code.

Loading the boot code using TFTP

1. Place the new boot code on a TFTP server to which the Brocade device has access.

2. Enter the following command at the privileged EXEC level of the CLI to copy the boot code from the TFTP server into flash memory:

   copy tftp flash *ip-addr image-file-name* bootrom

   For example:

   ```
   device# copy tftp flash 192.168.10.12 spz10106.bin bootrom
   ```

   ICX devices generate an output similar to the following:

   ```
   device# Load to buffer (8192 bytes per dot)
   ...............................................................................................
   SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT...
   ...............................................................................................
   TFTP to Flash Done
   ```

3. Verify that the code has been successfully copied by using the **show flash** command at any level of the CLI to check the boot code version. The output displays the compressed boot ROM code size and the boot code version.

Next, go to the section Loading the flash code using TFTP on page 24.

Loading the boot code using SCP

1. Place the new boot code on an SCP-enabled host to which the Brocade device has access.
2. If the device has only 8 MB of flash memory, or if you want to install a full Layer 3 image, delete both the primary and secondary image using the **erase flash** command.
3. Enter the following command to copy the boot code from the SCP-enabled host into flash memory:

   pscp *image-file-name hostname*@*management-ip*.flash:bootrom

   For example:

   ```
   C:\> pscp swz10106b002.bin terry@10.168.1.50:flash:bootrom
   ```

4. Verify that the code has been successfully copied onto the device by using the **show flash** command at any level of the CLI. The output displays the compressed boot ROM code size and the boot code version.

Next, go to the section Loading the flash code using SCP on page 26.

Loading the flash code using TFTP

The boot code is loaded.

> NOTE
> When upgrading the flash image version, the image is automatically updated across all stack units. For other devices, when upgrading from one major release to another (for example, from FastIron 8.0.30 to 8.0.40), make sure that every unit in the traditional stack has the same code. If you reboot the stack while units are running different code versions, the units cannot communicate.

1. Place the new flash code on a TFTP server to which the Brocade device has access.
2. If the device has only 8 MB of flash memory, or if you want to install a full Layer 3 image, make sure that the TFTP server and the image file are reachable and then delete the primary and secondary images before proceeding.

   If the primary flash contains additional files that are not related to the software update, it is recommended that these files also be deleted.

3. Copy the flash code from the TFTP server into flash memory using the **copy tftp flash** command.

   ```
   device# copy tftp flash 192.168.10.12 SPS08040.bin primary
   device# Load to buffer (8192 bytes per dot)
   .......................................................................
   .......................
   SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT...
   .......................................................................
   .......................
   TFTP to Flash Done.
   ```

   This example shows the loading of an image on an ICX 7450 or ICX 7750 device to primary flash memory.

4. Verify the flash image version by entering the **show flash** command.

   ```
   device# show flash
   Stack unit 1:
     Compressed Pri Code size = 24018046, Version:08.0.40qT213 (SPR08040q042.bin)
     Compressed Sec Code size = 24018046, Version:08.0.40qT213 (SPR08040q042.bin)
     Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215
     Code Flash Free Space = 1768706048
   device#
   ```

5. Reboot the device using the **reload** or **boot system** command.

   - Reboot the device by entering the **reload** command.

     ```
     device# reload
     ```

   - The following example shows how to boot the image from the secondary flash.

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

   - The following example shows how to boot the image from the primary flash and save the preference to the startup configuration.

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

6. Verify that the new flash image is running on the device by entering the **show version** command.

```
device# show version
Copyright (c) 1996-2015 Brocade Communications Systems, Inc. All rights
reserv
ed.
UNIT 1: compiled on Oct 1 2015 at 11:29:56 labeled as SPR08040q042
(24018046 bytes) from Secondary SPR08040q042.bin
SW: Version 08.0.40q042T213
Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215
(spz10105
b008)
Compiled on Thu Jul 16 06:27:06 2015
HW: Stackable ICX7450-24
Internal USB: Serial #: 9900614090900038
Vendor: ATP Electronics, Total size = 1919 MB
==========================================================================
UNIT 1: SL 1: ICX7450-24 24-port Management Module
Serial #:CYT3346K035
License: ICX7450_L3_SOFT_PACKAGE (LID: eavIIJLmFIK)
License Compliance: ICX7450-PREM-LIC-SW is Compliant for next 45 days
P-ASIC 0: type B548, rev 01 Chip BCM56548_A0
==========================================================================
UNIT 1: SL 2: ICX7400-4X10GF 4-port 40G Module
Serial #:CYV3346K07G
==========================================================================
UNIT 1: SL 3: ICX7400-1X40GQ 1-port 40G Module
Serial #:CYX3346K06F
==========================================================================
UNIT 1: SL 4: ICX7400-1X40GQ 1-port 40G Module
Serial #:CYX3346K00A
==========================================================================
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 0 day(s) 0 hour(s) 8 minute(s) 16 second(s)
The system : started=cold start
```

Loading the flash code using SCP

1. Place the new flash code on an SCP-enabled host to which the Brocade device has access.

2. Copy the flash code from the SCP-enabled host into the flash memory using the following methods.

   - Copy the flash code using SCP tool using the following command.

   scp *image-file-name hostname@management-ip*:**flash**:**primary** | **secondary**

   Or, if you also want to specify the name for the image file on the FastIron device, enter the following command:

   scp *image-file-name-on-scp-host hostname@management-ip*:**flash**:**pri** | **sec**:*image-file-name-on-device*

   > NOTE
   > The *image-file-name-on-device* variable is case-insensitive and converts any uppercase characters in the image file name to lowercase characters.

   For example:

   ```
   C:\> scp SPS08040.bin terry@10.168.1.50:flash:primary
   ```

   or

   ```
   C:\> scp SPS08040.bin terry@10.168.1.50:flash:pri:SPS08040.bin
   ```

   or

   ```
   C:\> scp SPS08040.bin terry@10.168.1.50:flash:secondary
   ```

   or

   ```
   C:\> scp SPS08040.bin terry@10.168.1.50:flash:sec:SPS08040.bin
   ```

   - Use PSCP to copy the flash code.

     pscp *image-file-name hostname@management-ip*:**flash**:**primary** | **secondary**

     ```
     D:\Images> pscp.exe SPS08040.bin terry@10.168.1.50:flash:primary
     ```

3. Verify that the flash code has been successfully copied onto the device by using the **show flash** command at any level of the CLI.

   ```
   device# show flash
   Stack unit 1:
     Compressed Pri Code size = 24018046, Version:08.0.40qT213 (SPR08040q042.bin)
     Compressed Sec Code size = 24018046, Version:08.0.40qT213 (SPR08040q042.bin)
     Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215
     Code Flash Free Space = 1768706048
   ```

4. Reboot the device using the **reload** or **boot system** command.

   ```
   device# reload
   ```

   or

   The following example shows how to set the system to boot the image from the secondary flash.

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

   or

   The following example shows how to set the system to boot the image from the primary flash and save the preference to the startup configuration.

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

5. Verify that the new flash image is running on the device by using the **show version** command.

```
device# show version
  Copyright (c) 1996-2015 Brocade Communications Systems, Inc. All rights
reserv                                                                          ed.
    UNIT 1: compiled on Oct  1 2015 at 11:29:56 labeled as SPR08040q042
      (24018046 bytes) from Secondary SPR08040q042.bin
        SW: Version 08.0.40q042T213
      Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215
(spz10105                                                                          b008)
       Compiled on Thu Jul 16 06:27:06 2015

  HW: Stackable ICX7450-24
  Internal USB: Serial #: 9900614090900038
      Vendor: ATP Electronics, Total size = 1919 MB
==========================================================================
UNIT 1: SL 1: ICX7450-24 24-port Management Module
      Serial  #:CYT3346K035
      License: ICX7450_L3_SOFT_PACKAGE   (LID: eavIIJLmFIK)
      License Compliance: ICX7450-PREM-LIC-SW is Compliant for next 45 days
      P-ASIC  0: type B548, rev 01  Chip BCM56548_A0
==========================================================================
UNIT 1: SL 2: ICX7400-4X10GF 4-port 40G Module
      Serial  #:CYV3346K07G
==========================================================================
UNIT 1: SL 3: ICX7400-1X40GQ 1-port 40G Module
      Serial  #:CYX3346K06F
==========================================================================
UNIT 1: SL 4: ICX7400-1X40GQ 1-port 40G Module
      Serial  #:CYX3346K00A
==========================================================================
 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 0 day(s) 0 hour(s) 8 minute(s) 16 second(s)
The system : started=cold start
```

Additional steps for loading boot code

There are additional steps for loading boot code on Brocade ICX 7250, ICX 7450, and ICX 7750 (ICX 7xxx) series devices.

The Brocade ICX 7xxx series devices hold a default boot code image and a backup boot code image. These two images are managed in a manner invisible to users. When boot code is downloaded during an upgrade, the boot code is downloaded to the backup boot code image. When the download is safely complete, the backup boot code image becomes the new default boot code image, and the former default boot code image becomes the new backup boot code image. The default boot code image is used by default for all subsequent reloads. The backup boot code is used when the default is unavailable for any reason.

To upgrade both boot code images, you must reload once between each download of boot code. it is necessary to reload one more time after the second download of boot code.

On ICX 7xxx series devices, Brocade recommends that you are certain that the default and backup boot code images hold the same version and are both bootable: To assure that both boot code images are bootable and hold the same version, when you perform any upgrade involving boot code, after the first reload with new code, download the same new boot code again, and reload once again.

You can use either the TFTP or SCP method for the additional download of new boot code. For example, with the TFTP method, after booting up a Brocade ICX 7450 with 8.0.30 and later for the first time, download compatible boot code using TFTP again, and reload once again in this manner:

```
device# copy tftp flash 192.168.10.12 spz10107.bin bootrom
....TFTP to Flash Done.
device# reload
Are you sure? (enter 'y' or 'n'): y
```

NOTE
File names vary for different releases.

For Brocade ICX 7xxx series devices, an alternative boot monitor download method is also available and is documented below.

Upgrading backup and default boot code images

Follow these steps to use the boot monitor method to upgrade Brocade ICX 7xxx series devices.

The boot monitor method for boot code download available to ICX 7250, ICX 7450, and ICX 7750 is similar to the software recovery method documented later in this upgrade guide. In the procedure below an ICX 7450 device is used.

NOTE
File names vary for different releases.

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.
3. On the TFTP server, assign an IP address to the connected NIC; for example, IP address 10.10.10.21 mask 255.255.255.0.
4. Reboot the device, and go to the boot monitor mode by pressing **b**.

```
U-Boot 10.1.04T215 (Oct 30 2014 - 00:08:19)
....
Enter 'b' to stop at boot monitor:
ICX7450-Boot> b
```

5. When in boot mode, enter the **printenv** command to display details of the environment variables available on the device memory.

```
ICX7450-Boot> printenv
baudrate=9600
ipaddr=192.168.60.13
serverip=192.168.60.1
netmask=255.255.255.0
gatewayip=192.168.0.1
uboot=spz10107
image_name=SPS08041.bin
ver=10.1.04T215 (Oct 30 2014 - 00:08:29)

Environment size: 183/16379 bytes
ICX7450-Boot>
```

6. Provide the IP address of the TFTP server that hosts a valid software image using the **setenv serverip** command.

```
ICX7450-Boot> setenv serverip 172.24.204.18
```

7. Set the IP address, netmask, and gateway IP address for the device management port.

   a) Set the IP address.

   ```
   ICX7450-Boot> setenv ipaddr 172.24.204.19
   ```

   b) Set the netmask.

   ```
   ICX7450-Boot> setenv netmask 255.255.255.0
   ```

   c) Set the gateway IP address.

   ```
   ICX7450-Boot> setenv gatewayip 172.24.204.1
   ```

   See the following section, Save the parameters configured in boot monitor on page 30.

8. Configure the filename of the boot code you intend to download.

   ```
   ICX7450-Boot> setenv uboot spz10107.bin
   ```

9. Download new boot code by entering the **update_uboot** command.

   ```
   ICX7450-Boot> update_uboot
   Loading image to Uboot Partition 2
   Using bcmiproc_eth-0 device
   TFTP from server 172.24.204.18; our IP address is 172.24.204.19
   Filename 'spz10107.bin'.
   Load address: 0x61007dc0
   Loading: ######################################################
   done
   Bytes transferred = 786944 (c0200 hex)
   sf erase 0x0 0x100000
   copying uboot image to flash, it will take sometime...
   sf write 0x61007fc0 0x0 0xc0000
   TFTP to Flash Done.
   ICX7450-Boot>
   ```

   The **update_uboot** command is unique to this upgrade method and it does not behave like any plain CLI TFTP download command.

10. Reload using either the **reset** or **powercycle** command. This allows you to boot using the newly downloaded boot code.

    -
      ```
      ICX7450-Boot> reset
      ```

    -
      ```
      ICX7450-Boot> powercycle
      ```

11. To upgrade the other boot code image, while the ICX is booting up again press **b** to enter boot monitor again, and continue from Step 4 above.

    ```
    U-Boot 10.1.04T215 (Oct 30 2014 - 00:09:11)
    ....
    Enter 'b' to stop at boot monitor:
    ICX7450-Boot> b
    ```

Save the parameters configured in boot monitor

In boot monitor, you can use the **saveenv** command to save values configured with the **setenv** command. However, caution is required when using the **saveenv** command from boot monitor after configuring an IP address with **setenv ipaddr**. Be aware of the following:

- If you use the **saveenv** command, the IP address you used in the command is configured the next time you enter boot monitor. However, after you boot up into flash code, even when that IP address does not appear in the running configuration, the ICX continues to respond to ARP requests for that IP address. The MAC address in those ARP replies will be a special boot monitor MAC address that is similar to but slightly different from the MAC addresses you can see with the **show interface** command.
- If you configure that same IP address on any other device in the same broadcast domain, you experience difficulty communicating with that other device.
- If you are using switching flash code on the ICX and you configure that same IP address in the running configuration, you will experience difficulty communicating with the ICX at that IP address.
- If you are using routing flash code on the ICX and you configure that same IP address on the management interface, the ICX will report a duplicate IP address detected on the management interface.

If you use **saveenv** after configuring **setenv ipaddr** in boot monitor, you must be careful to not use the same IP address anywhere else in your network even in the running configuration of the same ICX.

See the following section for the procedure to view the boot monitor IP parameters.

Viewing the boot monitor IP parameters

From the flash code CLI, it is possible to check the currently configured boot monitor IP address even though it does not appear in the running configuration.

1. Enter OS mode.

   ```
   ICX#  Press Ctrl+y, then the m key, then Enter
   Switch to OS console...
   ```

2. Check the configured boot monitor IP address.

   ```
   OS>show remote
     IP address      : 172.24.204.20
     subnet mask     : 255.255.255.0
     default gateway : 172.24.204.1
   ```

3. Return to the flash code CLI

   ```
   OS>  Press Ctrl+z
   Back to Application console...
   ICX#
   ```

View boot monitor IP parameters example

```
ICX# Press Ctrl+y, then the m key, then Enter
Switch to OS console...
OS> show remote
  IP address      : 172.24.204.20
  subnet mask     : 255.255.255.0
  default gateway : 172.24.204.1
OS> Press Ctrl+z
Back to Application console...
ICX#
```

Software upgrade using a manifest file

Manifest files are prepared for every release. They contain and list all boot, firmware, and application images as well as signature files. Brocade supports a manifest file software upgrade for both standalone devices and homogeneous stacks.

You can use a single command to copy boot and flash images. Using the official manifest file, the images are copied onto the devices, and all member units are upgraded. However:

- PoE Firmware must be upgraded manually after the manifest upgrade.
- Copying the manifest file using the SCP is not supported.
- For standalone devices or a homogeneous stack, the manifest upgrade process downloads the boot image to the device only if a newer boot image version is available.
- The manifest file specifies images for both router and switch types. Based on the device family and the type of image (switch or router), the appropriate images are installed.
- The command will only accept a manifest file with a .txt extension.

1. Ensure that the Brocade device has access to a TFTP server.
2. Determine the current software versions and license requirements then download the upgrade to a TFTP server, refer to Initial steps on page 19.

3. Unzip the downloaded FastIron image files on the TFTP server.

   This places the manifest file at the top of the directory structure with the images in subdirectories.

4. If upgrading from FastIron 8.0.10, delete the following lines from the manifest text file.

   ```
   -DIRECTORY /ICX7750/Boot
   swz10105.bin

   -DIRECTORY /ICX7750/Images
   SWS08030d.bin
   SWR08030d.bin

   -DIRECTORY /ICX7750/MIBs
   SWS08030d.mib
   SWS08030d.mib

   -DIRECTORY /ICX7750/Signatures
   SWR08030dnss.sig
   SWR08030d.sig
   SWS08030dnss.sig
   SWS08030d.sig
   swz10105nss.sig
   swz10105.sig

   -DIRECTORY /ICX7750/Manuals
   ```

   What is shown is when there is an upgrade to software release 8.0.30d. Depending on the upgrade, these lines may differ. If that is the case, just delete any lines under and including the -DIRECTORY /ICX7750/xxx headings.

5. On the Brocade device, enter one of the following commands to copy the manifest file and the images from the TFTP server:

   - **copy tftp system-manifest** *server-ip-address manifest-file-name* [**primary** | **secondary**]

     Or

   - **copy tftp system-manifest** *server-ip-address manifest-file-name* [**all-images-primary** | **all-images-secondary**]

   For example:

   ```
   device# copy tftp system-manifest 10.70.42.172 stage/FI08040_Manifest.txt primary
   ```

   You can use the all-images-primary and all-images-secondary options to copy all the images.

6. After all the relevant images have been installed on the device, you are prompted to reboot the device to complete the upgrade process.

   a) Execute the **write memory** command.

   b) Execute the **reload** command.

   The specified images are loaded to all 802.1br control bridge and port extender units.

The following example downloads all boot and application images for FastIron 8.0.40 from the TFTP server to an ICX 7750-26Q Router.

```
ICX7750-26Q Router# copy tftp system-manifest 10.70.42.172 stage/FI08040_Manifest.txt all-images-secondary

You are about to download boot image and boot signature image as well, ARE YOU SURE?(enter 'y' or 'n'): y
ICX7750-26Q Router#Flash Memory Write (8192 bytes per dot)
DOWNLOADING MANIFEST FILE   Done.
ICX7750-26Q Router#Flash Memory Write (8192 bytes per dot)
Automatic copy to member units:  3

COPY ICX7750 SIGNATURE TFTP to Flash Done
 ICX7750-26Q Router#Load to buffer (8192 bytes per dot)
Automatic copy to member units:  3
...
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
...
Copy ICX7750 from TFTP to Flash Done.
ICX7750-26Q Router#Flash Memory Write (8192 bytes per dot)
Automatic copy to member units:  3
...
DOWNLOAD OF ICX7750 BOOT SIGNATURE  Done.
ICX7750-26Q Router#Load to buffer (8192 bytes per dot)
Automatic copy to member units:  3
...
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
...
ICX7750 Boot IMAGE COPY IS DONE
 ICX7750-26Q Router#Load to buffer (8192 bytes per dot)
Automatic copy to member units: 17 18
...
PLEASE WAIT. MEMBERS SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT... Done.
ICX7750-26Q Router#Load to buffer (8192 bytes per dot)
Automatic copy to member units: 17 18
...
PLEASE WAIT. MEMBERS SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT...
  Manifest image download is complete, please reload the system
```

The following example copies the binary image for the FastIron 8.0.40 manifest file to secondary flash from the TFTP server to an ICX 7750-26Q Router.

```
ICX7750-26Q Router# copy tftp system-manifest 10.70.42.172 stage/FI08040_Manifest.txt secondary
ICX7750-26Q Router# Flash Memory Write (8192 bytes per dot) .....
DOWNLOADING MANIFEST FILE   Done.
ICX7750-26Q Router#Flash Memory Write (8192 bytes per dot)
Automatic copy to member units:  3
...
COPY ICX7750 SIGNATURE TFTP to Flash Done
 ICX7750-26Q Router# Load to buffer (8192 bytes per dot)
Automatic copy to member units:  3
...
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
...
Copy ICX7750 from TFTP to Flash Done.
ICX7750-26Q Router#Load to buffer (8192 bytes per dot)
Automatic copy to member units: 17 18
...
PLEASE WAIT. MEMBERS SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT...
Copy ICX7450 from TFTP to Flash Done.

Manifest file upgrade done, please reload the system
```

Example of a manifest file upgrade

The following example downloads all boot and application images for FastIron 08.0.40 from the TFTP server.

```
device# copy tftp system-manifest 10.70.42.172 stage/FI08040_Manifest.txt all-images-secondary

You are about to download boot image and boot signature image as well, ARE YOU SURE?(enter 'y' or 'n'): y
```

```
device#Flash Memory Write (8192 bytes per dot)
DOWNLOADING MANIFEST FILE   Done.
device#Flash Memory Write (8192 bytes per dot)
Automatic copy to member units:  3

COPY ICX7750 SIGNATURE TFTP to Flash Done
 device#Load to buffer (8192 bytes per dot)
Automatic copy to member units:  3
...
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
...
Copy ICX7750 from TFTP to Flash Done.
device#Flash Memory Write (8192 bytes per dot)
Automatic copy to member units:  3
...
DOWNLOAD OF ICX7750 BOOT SIGNATURE  Done.
device#Load to buffer (8192 bytes per dot)
Automatic copy to member units:  3
...
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
...
ICX7750 Boot IMAGE COPY IS DONE
 device#Load to buffer (8192 bytes per dot)
Automatic copy to member units: 17 18
...
PLEASE WAIT. MEMBERS SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT... Done.
device#Load to buffer (8192 bytes per dot)
Automatic copy to member units: 17 18
...
PLEASE WAIT. MEMBERS SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT...
  Manifest image download is complete, please reload the system
```

Boot from USB

Software upgrade can be done through manifest file download using a USB drive. The following actions must be performed to initiate the corresponding control flow for booting from USB.

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.

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 to have only one manifest file set in the USB drive. 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 should be a different version than in the system flash memory. If an error occurs during the auto-copy process, the system aborts booting from USB.

> NOTE
> Configuration file must be deleted from the system using the **erase startup-configuration** command. Booting from 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 bootup, 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 example "ICX7650.cfg,"ICX7150.cfg"
- “brocade.cfg”

Booting from 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
Booting from USB is supported only on ICX 7150 and ICX 7650.

NOTE
Booting from USB is not supported on SPX.

The USB status mode LED indicates the status of boot from USB and is described in the *Ruckus ICX 7650 Switch Hardware Installation Guide*.

System backup to USB

You can copy files from the system flash memory to the connected USB drive. The feature is disabled by default and you must enable it using the **reverse-manifest-enable** command in global configuration mode. To initiate system backup to USB, you must plug in the USB drive when the system is up and running, and press and hold the USB mode button for 10 seconds. This action triggers system backup to USB and the manifest files, image files, boot loader, signature file, configuration files, and supportsave files are copied to the connected USB drive. The system backup to USB can be triggered any number of times and each time the existing files will be overwritten with new files.

NOTE
An additional 70 MB in the USB drive must be available for all the files to be copied during reverse USB manifest.

There may be instances in which the image and boot files are loaded to the system using a TFTP or SCP download instead of a manifest file. In such cases, manifest files are not available and must be generated. If an error occurs during file copy, the system aborts the system backup operation.

The USB status mode LED indicates the different status of system backup and is described in the *Ruckus ICX 7650 Switch Hardware Installation Guide*.

System backup to USB is supported only on a standalone unit, stack master, active CB, and PE unit. System backup to USB is not applicable on standby and member units.

NOTE
System backup to USB on SPX configurations is not supported for FastIron 08.0.70 release.

Software recovery

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

```
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
```

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 Brocade support engineer.

Recovering software

> NOTE
> In practice, the TFTP server is also used as the terminal server to see the CLI output.

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.
3. On the TFTP server, assign an IP address to the connected NIC. For example enter:

   ```
   IP address 10.10.10.21 mask 255.255.255.0
   ```

4. Reboot the device.
5. When in boot mode, enter the **printenv** command to display details of the images available on the device memory. For example:

   ```
   ICX7450-boot> printenv
   baudrate=9600
   uboot=brocade/ICX7450/bootcode/spz10106b002
   Version:10.1.06T215 (May  15 2015 - 11:28:23)
   ```

   The path is to the boot image on the TFTP server.
6. Provide the IP address of the TFTP server that hosts a valid software image using the **setenv serverip** command. For example:

   ```
   ICX7450-boot> setenv uboot 10.10.10.21
   ```

7. 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. For example:

   ```
   ICX7450-boot> setenv ipaddr 10.10.10.22
   ICX7450-boot> setenv gatewayip 10.10.10.1
   ICX7450-boot> setenv netmask 255.255.255.0
   ICX7450-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.

8. Enter the **printenv** command to verify the IP addresses that you configured for the device and the TFTP server. For example:

   ```
   ICX7450-boot> printenv
   baudrate=9600
   ipaddr=10.10.10.22
   gatewayip=10.10.10.1
   netmask=255.255.255.0
   serverip=10.10.10.1
   uboot=brocade/ICX7450/bootcode/spz10106b002
   Version:10.1.06T215 (May  15 2015 - 11:28:23)
   ```

9. Test the connectivity to the TFTP server from the device using the **ping** command to ensure a working connection. For example:

```
ICX7450-boot> ping 10.10.10.21
ethPortNo = 0
Using egiga0 device
host 10.10.10.21 is alive
```

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

```
ICX7450-boot> setenv image_name images/ICX/SPR08040.bin
```

11. Update the primary flash using the **update_primary** command. For example:

```
ICX7450-boot> update_primary
ethPortNo = 0
Using egiga0 device
TFTP from server 10.10.10.21; our IP address is 10.10.10.22
Download Filename 'SPR08040.bin'.
Load address: 0x3000000
Download to address: 0x3000000
Loading: %#################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         ########################################################
done
Bytes transferred = 10360844 (9e180c hex)
prot off f8100000 f907ffff
................................................................................
................................................................................
................................................................................
........
Un-Protected 248 sectors
erase f8100000 f907ffff
.................................................
.................................................................
.................................................................
.................................................................
....
Erased 248 sectors
copying image to flash, it will take sometime...
sflash write 3000000 100000 f80000
TFTP to Flash Done.
```

12. Load the image from the primary flash using the **boot_primary** command; for example:

```
ICX7450-boot> boot_primary
Booting image from Primary
## Booting image at 00007fc0 ...
   Created:      2015-05-02  20:38:52 UTC
   Data Size:    10360268 Bytes =  9.9 MB
   Load Address: 00008000
   Entry Point:  00008000
   Verifying Checksum ... OK
OK
Starting kernel in BE mode ...
Uncompressing Image.............................................................
................................................................................
................................................................................
................................................................................
................................................................................
........................................... done, booting the kernel.
Config partition mounted.
```

13. Enter **show flash** and see the output to check whether the image copy process was successful.
14. Copy the image from the primary to the secondary flash partition using the **copy flash flash secondary** command.

Downgrade process

Before downgrading the software on the device, refer to Upgrade and Downgrade Considerations on page 11. In general, before a downgrade, keep these points in mind:

- IPv6 static routing - If you downgrade from FastIron 8.0.40 to a release that is covered by a premium license, there is no impact. If the earlier release is not covered by a premium license, any IPv6 static routing configuration is lost.
- SSHv2 RSA - Host key format may differ among FastIron software versions.
- Pre 8.0.10 releases - If the downgrade is to a version earlier than FastIron 8.0.10, software-based licensing is not supported.
- There are changes in behavior of:
  - Flexible authentication
  - Command line interface

In-service software upgrade

An in-service software upgrade (ISSU) allows stack units or units in a Campus Fabric (SPX) system to be upgraded with minimal interruptions to multi-unit topologies.

ISSU provides an incremental method to upgrade traditional stacks and Campus Fabric (SPX) systems. 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.

NOTE
Traffic through PE nodes is affected by ISSU because PE ports cannot be part of a traditional LAG.

ISSU limitations and considerations

When using ISSU, consider the following:

- ISSU is supported on FastIron ICX 7150, ICX 7250, ICX 7450, and ICX 7750 stackable hardware.

- ISSU is supported in a homogenous ring stack topology and an SPX topology where control bridges are connected in a ring. PE units can be connected in either linear or ring topologies.
- ISSU works for stacks of two units to the maximum supported twelve units.
- ISSU is supported in SPX configurations with the maximum number of PE units.
- ISSU is supported for upgrades between minor releases only. For example, you can use ISSU to upgrade between 08.0.70 and 08.0.70a but not between 08.0.70 and 08.0.80.
- For ISSU to occur with minimal disruption, the customer network connected to the stack and CB units in an SPX system 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
  - Stack commands or SPX commands that may result in topology change or discovery
  - Initiation of another ISSU
  - New PE join activity

The following additional items are blocked during ISSU in a Campus Fabric system:

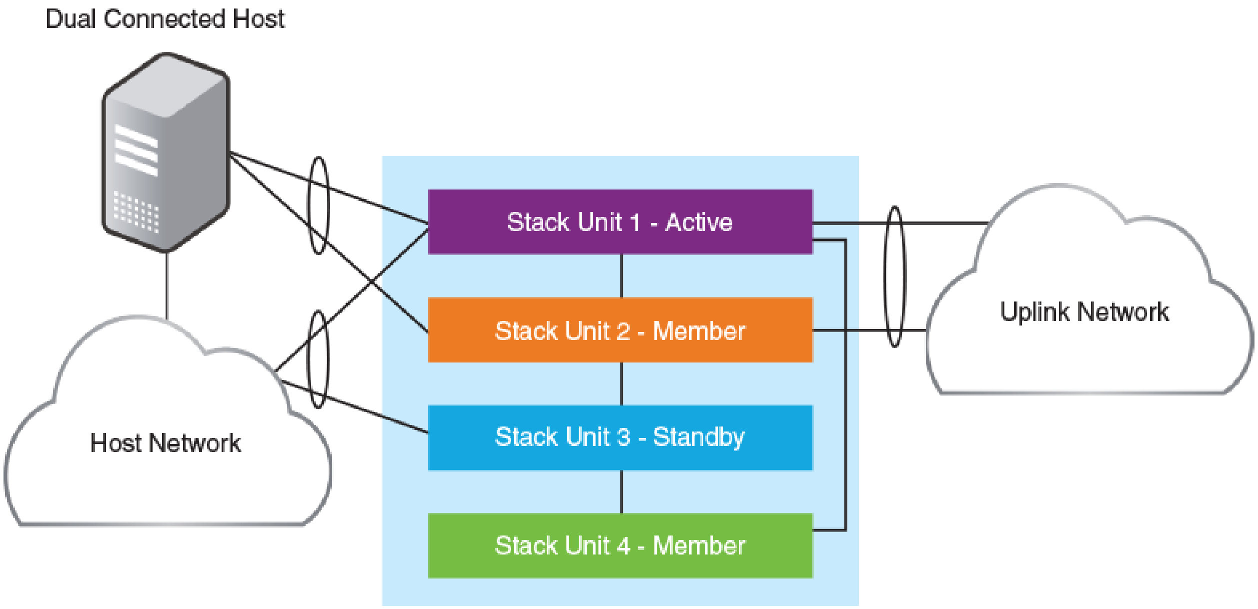
- The web interface
- SPX DDM commands
- SPX interactive-setup
- SPX zero-touch provisioning
- Clear commands

ISSU recommended stack topology

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 1 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.

ISSU recommended SPX topology

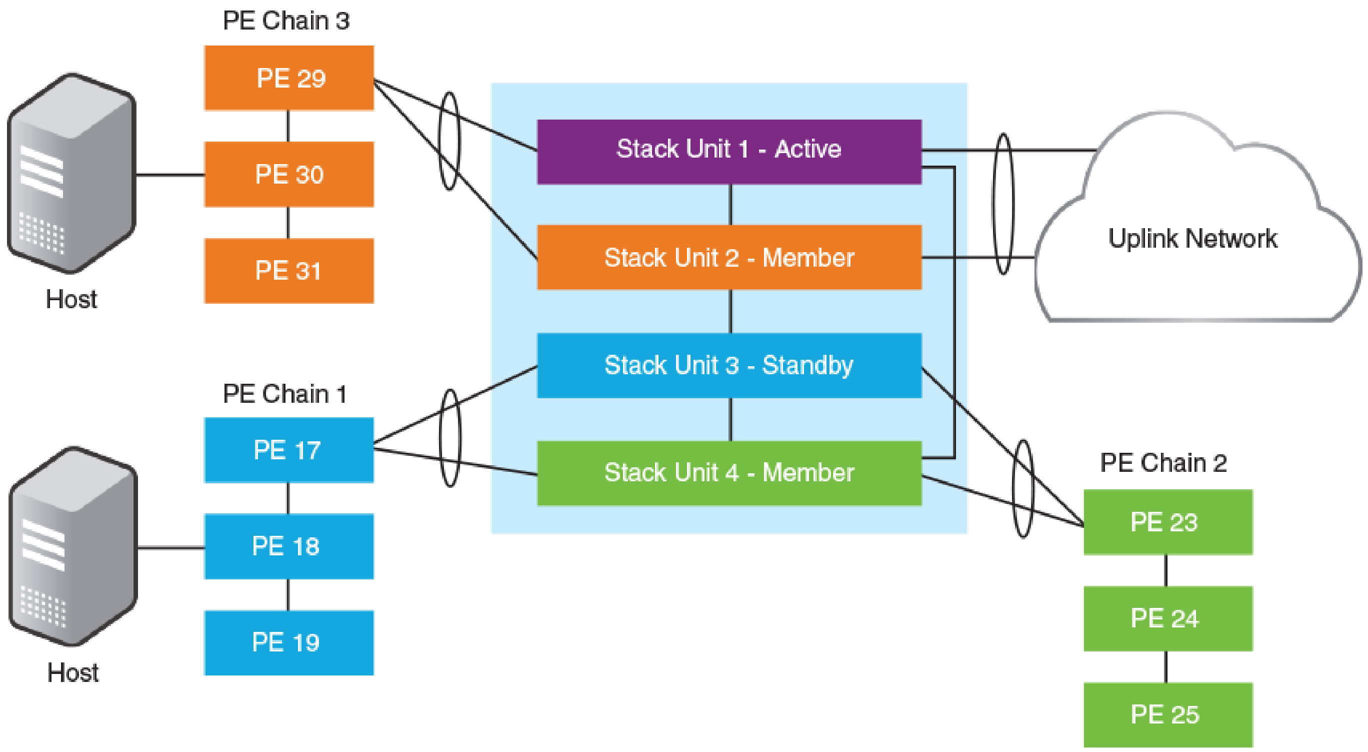
ISSU provides the ability to upgrade SPX systems with minimal traffic loss.

Multi-PE unit LAGs are not supported in an SPX system, which means that traffic through a PE being upgraded is affected by the upgrade. ISSU reduces the network impact of an upgrade only if redundant uplink and downlink connections are available from multiple CB stack units.

NOTE
Because traditional LAGs are not supported on PE units in an SPX system, dual connectivity (through two different PE units) is recommended for every PE chain or ring.

The following figure illustrates a typical topology where ISSU can be used effectively to upgrade an SPX system.

FIGURE 2 Recommended topology for SPX ISSU



In the figure, redundant links connect different CB units in the SPX system to the uplink network. As each node is upgraded, it undergoes a hardware reset, which resets the packet processor and disrupts traffic flowing through the node. The redundant links allow traffic to flow through other units, minimizing the impact of each unit upgrade.

How ISSU works when upgrading stack units

The following set of steps describes the pre-checks and the upgrade sequence for an 8-unit stack in a typical topology.

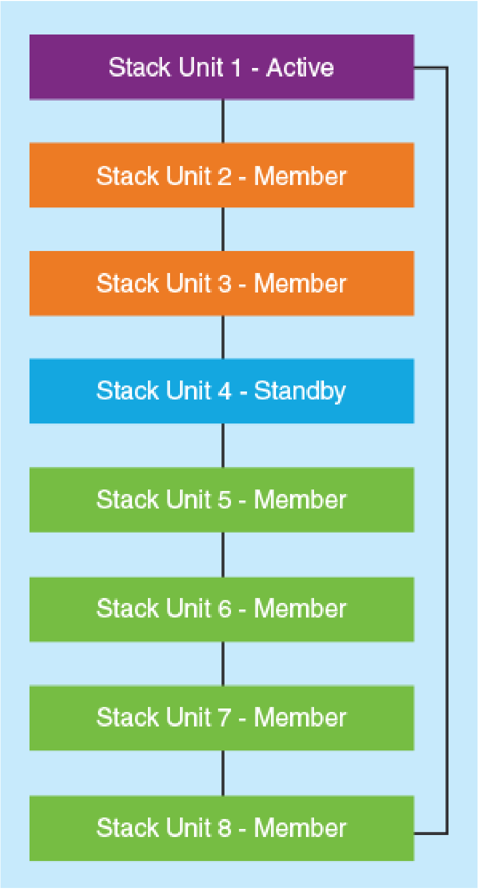
1. Use the **copy tftp** command to copy the image to the primary or secondary partition.
2. Use the **show issu status** command to check for upgrade readiness and the **show issu sequence** command to check the upgrade sequence.
3. Use the **issu primary** command or the **issu secondary** command to initiate the process.

The system responds to the command as follows:

- 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 unit (4, 3, 2 in the following figure) reload the new image.
- All members from standby controller to active controller in the other direction (6, 7, 8) 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.

FIGURE 3 Stack units to be upgraded



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.

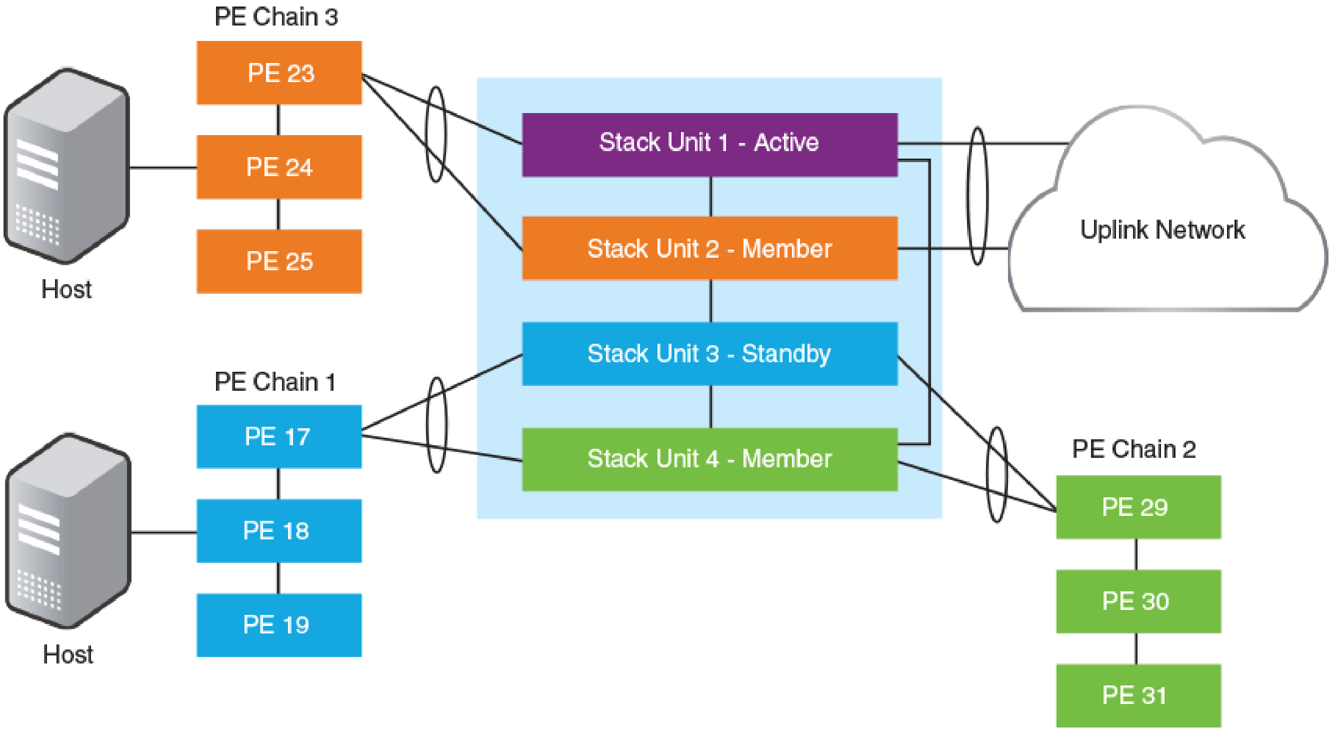
How ISSU works when upgrading an SPX system

The following set of steps describes the pre-checks and the upgrade sequence for an SPX system in a typical topology.

1. Use the **copy tftp** command to copy the image to the primary or secondary partition of the CB units.
2. Use the **copy tftp** command to copy the image to the same partition on the PE units as in the previous step.
3. Use the **show issu status** command to check for upgrade readiness and the **show issu sequence** command to check the upgrade sequence.

   The output of the **show issu sequence** command for the following SPX topology appears beneath the following figure.

FIGURE 4 Typical SPX topology



```
ICX7750-48F Router# show issu sequence
Stack units will be upgraded in the following order
ID      Type            Role
3       ICX7750-48XGC   standby
   17   ICX7450-32ZP    spx-pe
   18   ICX7150-48ZP    spx-pe
   19   ICX7150-48      spx-pe
2       ICX7750-20QXG   member
   23   ICX7450-32ZP    spx-pe
   24   ICX7150-48ZP    spx-pe
   25   ICX7150-48      spx-pe
4       ICX7750-48XGF   member
   29   ICX7450-32ZP    spx-pe
   30   ICX7150-48ZP    spx-pe
   31   ICX7150-48      spx-pe
1       ICX7750-48XGF   active

PEs 17, 18, 19 are associated with CB unit 3 for upgrade.
PEs 23, 24, 25 are associated with CB unit 2 for upgrade.
PEs 29, 30, 31 are associated with CB unit 4 for upgrade.
```

PE units are upgraded along with their associated CB units. This association of PE units to CB units is computed automatically.

4. Enter the **issu primary** command or the **issu secondary** command, including one of the on-error options, to initiate the process.

   NOTE
   It is recommended that you use one of the on-error options available with the issu commands to ensure graceful restart in the unlikely even of an ISSU failure. Refer to the section Error recovery on page 54 for additional information.

   NOTE
   If the **issu secondary** command is used, the default boot partition for the SPX system is set as secondary on successful completion of the ISSU process.

The system responds to the command as follows:

- Unit 3, the standby controller, is reloaded with the new image, along with associated PEs 17, 18, and 19.
- Once the standby controller and associated PEs join the SPX system, member units from the standby controller to the active controller (unit 2 in the previous figure) reload from the new image. Along with CB unit 2, associated PEs 23, 24, and 25 are also upgraded.
- All members from standby controller to the active controller in the other direction (unit 4) reload from the new image. Along with unit 4, associated PEs 29, 30, and 31 are also upgraded.
- Once all member units and the standby controller are reloaded with the new image, the active controller triggers a switchover, in which the old standby controller (unit 3) becomes the new active controller, and the old active controller (unit 1) becomes the new standby controller.
- The new active controller (unit 3) reloads the old active controller (unit 1) with the new image. If there are any PEs attached to unit 3 that are not yet upgraded (none in this example), they are upgraded next.
- Once the old active controller (unit 1) comes up as a member unit and rejoins the SPX system, standby controller election occurs, and the SPX system becomes fully functional with the upgraded image.

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

Upgrading a stack with ISSU

Complete the following steps to upgrade a stack using ISSU.

By default, switches are booted from the primary partition.

> NOTE
> The following examples for copying images represent typical use. Other options such as manifest-based image copy can also be used.

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

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

   b) Copy the new image to the primary partition.

   ```
   device# copy tftp flash 10.10.10.10 SWR08050.bin primary
   ```

   The IP address is for the TFTP server. It 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
   ```

3. Initiate the upgrade.

   - Initiate the upgrade without error recovery.

     ```
     device# issu secondary
     Stack opology is Ring                    Yes
     Standby Present                          Yes
     Standby ready for upgrade                Yes
     Flash use in progress                    No
     PoE-firmware upgrade in progress         No
     Secure 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
     Startup config and Running Config Same   Yes
     User in Config mode                      No
     Proceed with upgrade? (enter 'y' or 'n'):
     ```

     If an error occurs, the error condition is marked by three asterisks.

     ```
     device# issu primary
     Topology is Ring                         Yes
     Standby Present                          No   ***
     Standby ready for upgrade                No   ***
     Flash use in progress                    No
     Secure 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
     User in Config mode                      No
     System not ready for issu. Check error condition highlighted by "***" and rectify.
     ISSU not in progress
     ```

   - Initiate the upgrade with error recovery.

     ```
     device# issu primary on-error reload-primary
     Topology is Ring                         Yes
     Standby Present                          Yes
     Standby ready for upgrade                Yes
     Flash use in progress                    No
     Secure 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
     Startup config and Running Config Same   Yes
     User in Config mode                      No
     Proceed with upgrade? (enter 'y' or 'n'):
     ```

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

4. Check the status of an upgrade.

   Status display with an uninterrupted upgrade:

   ```
   ddevice# 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
   ```

   Status display with 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
   ```

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

5. Wait for the upgrade to complete.

   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 2016
   The older image before-ISSU SPR08060.bin
   Topology is Ring Yes
   Standby Present Yes
   Standby ready for upgrade Yes
   Flash use in progress No
   Secure 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
   User in Config mode No
   System ready for issu
   ISSU not in progress
   ```

   The following example shows an unsuccessful ISSU that was aborted due to a hotswap 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
    Secure 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
    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 with no **on-error** option), the stack is left as it is, and a manual recovery is required.

Brief ISSU command example for upgrading a stack

```
device# copy flash flash secondary
device# copy tftp flash 10.10.10.10 SWR08050.bin primary
device# show issu sequence
device# issu primary on-error reload-primary
device# show issu status
```

Upgrading an SPX system with ISSU

Follow these steps to upgrade an SPX system using ISSU.

NOTE
By default, FastIron devices are booted from the primary partition.

NOTE
The IP address used in the following code examples (10.10.10.10) is for the TFTP server. The address may be an IPv4 or an IPv6 address. The .bin file names used in the examples are image file names.

1. Copy the images.

   a) Back up the running image on the CB to the secondary partition.

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

   b) Back up the running image on the PE to the secondary partition.

   ```
   device# copy tftp flash 10.10.10.10 SPR08070.bin secondary
   ```

   c) Copy the new image to the primary partition on the CB.

   ```
   device# copy tftp flash 10.10.10.10 SWR08070.bin primary
   ```

   d) Copy the new image to the partition on the PE.

   ```
   device# copy tftp flash 10.10.10.10 SPR08070.bin primary
   ```

2. Check the sequence of the upgrade.

   ```
   device# show issu sequence

   Stack units will be upgraded in the following order
   ID   Type             Role
    2    ICX7750-20QXG     standby
    3    ICX7750-48XGF     member
   20    ICX7150-48PF      spx-pe
   21    ICX7150-48P       spx-pe
   22    ICX7150-48P       spx-pe
   18    ICX7450-24G       spx-pe
   19    ICX7450-24G       spx-pe
    1    ICX7750-20QXG     active
   17    ICX7450-24G       spx-pe
   ```

3. Initiate the upgrade.

   - Initiate the upgrade without error recovery.

```
device# issu secondary
Topology is Ring                         Yes
Standby Present                          Yes
Standby ready for upgrade                Yes
Flash use in progress                    No
Secure Setup in progress                 No
Spx interactive-setup in progress        No
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
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'):
```

NOTE
If an error occurs, the error condition is marked by three asterisks.

```
device# issu primary
Topology is Ring                         Yes    ***
Standby Present                          Yes    ***
Standby ready for upgrade                Yes
Flash use in progress                    No
Secure Setup in progress                 No
Spx interactive-setup in progress        No
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
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.
```

   - Initiate the upgrade with error recovery.

```
device# issu primary on-error reload-primary
Topology is Ring                         Yes
Standby Present                          Yes
Standby ready for upgrade                Yes
Flash use in progress                    No
Secure Setup in progress                 No
Spx interactive-setup in progress        No
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
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'):
```

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

4. Use the **show issu status** command to check ISSU status.

   If the upgrade has not been initiated, the command displays information on whether the system is ready for upgrade.

```
device# show issu status
ISSU Status: In Progress
Upgrade State: UNIT TO BE UPGRADED
Upgrade Option: issu primary on-error reload-primary

ID   Type          Role      State
2    ICX7750-20QXG standby   UPGRADE PENDING
3    ICX7750-48XGF member    UPGRADE PENDING
20   ICX7150-48PF  spx-pe    UPGRADE PENDING
21   ICX7150-48P   spx-pe    UPGRADE PENDING
22   ICX7150-48P   spx-pe    UPGRADE PENDING
18   ICX7450-24G   spx-pe    UPGRADE PENDING
19   ICX7450-24G   spx-pe    UPGRADE PENDING
1    ICX7750-20QXG active    UPGRADE PENDING
17   ICX7450-24G   spx-pe    UPGRADE PENDING
```

   The previous example displays status of an uninterrupted 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
2    ICX7750-20QXG standby   UPGRADE ABORT
3    ICX7750-48XGF member    UPGRADE PENDING
20   ICX7150-48PF  spx-pe    UPGRADE PENDING
21   ICX7150-48P   spx-pe    UPGRADE PENDING
22   ICX7150-48P   spx-pe    UPGRADE PENDING
18   ICX7450-24G   spx-pe    UPGRADE PENDING
19   ICX7450-24G   spx-pe    UPGRADE PENDING
1    ICX7750-20QXG active    UPGRADE PENDING
17   ICX7450-24G   spx-pe    UPGRADE PENDING
```

   The previous example displays an aborted upgrade.

5. Wait for the upgrade to complete.

   NOTE
   If the upgrade is aborted manually, or if the ISSU process detects an abort condition (when the **issu** command is executed with no **on-error** option), the stack is left as it is, and a manual recovery is required.

Upgrading an SPX system with ISSU

The following ISSU example includes an error recovery option.

```
device# copy flash flash secondary
device# copy tftp flash 10.10.10.10 SPR08070.bin secondary
device# copy tftp flash 10.10.10.10 SWR08070.bin primary
device# copy tftp flash 10.10.10.10 SPR08070.bin primary
device# show issu sequence
Stack units will be upgraded in the following order
ID     Type              Role
 2      ICX7750-20QXG     standby
 3      ICX7750-48XGF     member
20      ICX7150-48PF      spx-pe
21      ICX7150-48P       spx-pe
22      ICX7150-48P       spx-pe
18      ICX7450-24G       spx-pe
19      ICX7450-24G       spx-pe
 1      ICX7750-20QXG     active
17      ICX7450-24G       spx-pe

device# issu primary on-error reload-primary
Topology is Ring                         Yes
Standby Present                          Yes
Standby ready for upgrade                Yes
Flash use in progress                    No
Secure Setup in progress                 No
Spx interactive-setup in progress        No
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
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'): y

device# show issu status
ISSU Status: In Progress
Upgrade State: UNIT TO BE UPGRADED
Upgrade Option: issu primary on-error reload-primary

ID   Type          Role      State
2    ICX7750-20QXG standby   UPGRADE PENDING
3    ICX7750-48XGF member    UPGRADE PENDING
20   ICX7150-48PF  spx-pe    UPGRADE PENDING
21   ICX7150-48P   spx-pe    UPGRADE PENDING
22   ICX7150-48P   spx-pe    UPGRADE PENDING
18   ICX7450-24G   spx-pe    UPGRADE PENDING
19   ICX7450-24G   spx-pe    UPGRADE PENDING
1    ICX7750-20QXG active    UPGRADE PENDING
17   ICX7450-24G   spx-pe    UPGRADE PENDING
```

Pre-ISSU compatibility check

After the image is downloaded to flash and ISSU is triggered, but before ISSU processing begins, a pre-ISSU compatibility check is executed.

The compatibility check examines and reports either Yes (the stack is ready in this regard for an upgrade) or No (the stack is not ready for an upgrade). A successful compatibility check displays the passing results shown in the following table.

TABLE 7 Pre-ISSU checks for a traditional stack

Check	Passing result
All units in ready state	Yes
Standby present	Yes
Standby ready for upgrade	Yes
Stack topology is ring	Yes
PoE-firmware download in progress	No
Flash use in progress	No
ISSU in progress or aborted	No
Secure setup in progress	No
Election pending	No
Election in progress	No
Reload pending	No
CPU utilization high	No
Primary image is upgrade compatible	Yes
Secondary image is upgrade compatible	Yes
Startup configuration and running configuration same	Yes
Boot option present in running configuration	Yes
SPX interactive setup in progress	No
Zero-touch provisioning configured	No
User in configuration mode	No

NOTE
An error condition is indicated by three asterisks (***).

Typical reasons for the failure of a pre-ISSU image compatibility check (primary or secondary) include (in order of occurrence):

1. Redesign of application functionality.
2. Redesign of application sync functionality.
3. Software architecture changes.
4. System-max changes.

Pre-ISSU checks in an SPX system

Before an ISSU is performed in an SPX system, a set of checks similar to the set of compatiblity checks performed for a stack is executed. The following table lists pre-ISSU requirements for an SPX system. Any differences between an SPX system and a stacking system are noted.

NOTE
In contrast to the standard stacking checklist, Zero-touch provisioning (ZTP) cannot be in progress when an SPX ISSU is initiated.

TABLE 8 Pre-ISSU checks for an SPX system

Check	Passing result
All units in ready state	Yes
Standby present	Yes
Standby ready for upgrade	Yes

TABLE 8 Pre-ISSU checks for an SPX system (continued)

Check	Passing result
Stack topology is ring	Yes
PoE-firmware download in progress	No
Flash use in progress	No
ISSU in progress or aborted	No
Secure setup in progress	No
Election pending	No
Election in progress	No
Reload pending	No
CPU utilization high	No
Primary image is upgrade compatible	Yes
Secondary image is upgrade compatible	Yes
Startup configuration and running configuration same	Yes
Boot option present in running configuration	No
SPX CB Mode enabled	Yes (unique to SPX ISSU)
SPX interactive-setup in progress	No
Zero-touch provisioning configured	No
User in configuration mode	No

ISSU errors

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

TABLE 9 Common errors

Error message	Description
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 or SPX system within the specified time after an upgrade.
Unit delete	The unit is detached from the stack or SPX system while the ISSU is in progress.
Ping fail	A unit fails to respond to keepalive messages.

TABLE 10 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 The active controller detects this condition as a unit delete and reloads all the existing stack members from the par **error** option.
Active reload/crash	If the active controller reloads unexpectedly, or crashes while the ISSU is in progress, the stack units detect the los ISSU. If the **issu** command **on-error** option is specified, all units that were part of the stack at the time of the active contr partition specified in the command. Any units that were being upgraded at the time of the active controller failover the **issu** command.

TABLE 10 Crash and manual abort errors (continued)

Error message	Description
	Once all units have booted and an active controller has been elected, if some units have a running image different t **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 m 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:

- If ISSU is started with the **issu primary** or **issu secondary** command:
  - 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 the topic 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

Follow these 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
   ```

Reverting to the old image

Once the upgrade is completed, the primary partition has the new image, and the secondary partition has the older image. You can use the following steps to move the stack back to the older image.

1. Move the older image from the secondary partition to the primary partition.
   - For a traditional stack, use the following command.

     ```
     device# copy flash flash primary
     ```

   - For an SPX system, use the following command for CB units.

     ```
     device# copy flash flash primary
     ```

   - For an SPX system, use the following command for PE units.

     ```
     device# copy tftp flash 10.10.10.10 SPR08070.bin primary
     ```

2. Confirm that the proper image has been reloaded on all units.
3. Reboot the system from the primary flash image.

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

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com