Junos® OS

Installation and Upgrade Guide

Release
14.1

Modified: 2016-06-17

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Installation and Upgrade Guide
14.1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- ACX Series
- M Series
- MX Series
- T Series
- J Series
- EX Series
- PTX Series
- QFabric System

- QFX Series standalone switches
- SRX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xxii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xxii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Junos Software and Hardware Overview

CHAPTER 1

Software Overview

Junos OS Overview

Juniper Networks provides high-performance network devices that create a responsive and trusted environment for accelerating the deployment of services and applications over a single network. The Junos® operating system (Junos OS) is the foundation of these high-performance networks. Unlike other complex, monolithic software architectures, Junos OS incorporates key design and developmental differences to deliver increased network availability, operational efficiency, and flexibility. The key advantages to this approach are:

One Operating System

Unlike other network operating systems that share a common name but splinter into many different programs, Junos OS is a single, cohesive operating system that is shared across all network devices and product lines. This allows Juniper Networks engineers to

develop software features once and share these features across all product lines simultaneously. Because features are common to a single source, they generally are implemented the same way for all product lines, thus reducing the training required to learn different tools and methods for each product. Because all Juniper Networks products use the same code base, interoperability between products is not an issue.

One Modular Software Architecture

Although individual modules of Junos OS communicate through well-defined interfaces, each module runs in its own protected memory space, preventing one module from disrupting another. This separation enables the independent restart of each module as necessary. This is in contrast to monolithic operating systems where a malfunction in one module can ripple to other modules and cause a full system crash or restart. This modular architecture then provides for high performance, high availability, security, and device scalability not found in other operating systems.

The Junos OS is preinstalled on your Juniper Networks device when you receive it from the factory. Thus, when you first power on the device, all software starts automatically. You simply need to configure the software so that the device can participate in the network.

You can upgrade the device software as new features are added or software problems are fixed. You normally obtain new software by downloading the software installation packages from the Juniper Networks Support Web page onto your device or onto another system on your local network. You then install the software upgrade onto the device.

Juniper Networks routing platforms run only binaries supplied by Juniper Networks, and currently do not support third-party binaries. Each Junos OS image includes a digitally signed manifest of executables that are registered with the system only if the signature can be validated. Junos OS will not execute any binary without a registered signature. This feature protects the system against unauthorized software and activity that might compromise the integrity of your device.

Related Documentation

- Junos OS Editions on page 4
- Junos OS Installation Packages on page 5

Junos OS Editions

Junos OS is released in the following editions:

- Domestic—Junos OS for customers in the United States and Canada, and for all other customers with a valid encryption agreement. This edition includes high-encryption capabilities such as ipsec and ssh for data leaving the router or switch.
- Export—Junos OS for all other customers. This edition does not include any high-encryption capabilities for data leaving the router or switch.
- Junos-FIPS—Junos OS that provides advanced network security for customers who need software tools to configure a network of Juniper Networks routers and switches in a Federal Information Processing Standards (FIPS) 140-2 environment. For more information about Junos-FIPS, see "FIPS 140-2 Security Compliance" on page 5.

FIPS 140-2 Security Compliance

For advanced network security, a special version of Junos OS, called Junos-FIPS 140-2, is available. Junos-FIPS 140-2 provides customers with software tools to configure a network of Juniper Networks devices in a FIPS environment. FIPS support includes:

- Upgrade package to convert Junos OS to Junos-FIPS 140-2
- Revised installation and configuration procedures
- Enforced security for remote access
- FIPS user roles (Crypto Officer, User, and Maintenance)
- FIPS-specific system logging and error messages
- IPsec configuration for Routing Engine–to–Routing Engine communication
- Enhanced password creation and encryption

Junos-FIPS has special installation and configuration requirements. Installation procedures include downloading the FIPS software package from **www.juniper.net**. For detailed guidelines on how installation and configuration procedures differ between Junos OS and Junos-FIPS 140-2, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

NOTE: **Junos-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the device, you cannot configure passwords unless they meet this standard.**

Junos OS Installation Packages

The installation package is used to upgrade and downgrade from one release to another. When installed, the installation package completely reinstalls the software, rebuilds the Junos OS file system, and may erase system logs and other auxiliary information from the previous installation. The installation package does, however, retain the configuration files from the previous installation.

The following installation packages are available for download:

Installation Package	Description
jinstall*	Junos OS for the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers.
jinstall-ex*	Junos OS for the EX Series Ethernet Switch portfolio.
junos-jsr*	Junos OS for the J Series routers.

junos-juniper*	Junos-FIPS for the M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers. Once the package is installed on a device, you cannot revert back to the standard Junos OS installation without performing a software recovery procedure.
jinstall64*	64-bit Junos OS for the JCS1200 Route Reflector, TX Matrix Plus routers with 3D SIBs, and PTX Series Packet Transport Routers.
junos-srxsme*	Junos OS for all the branch SRX Series.
junos-srx1k3k*	Junos OS for SRX1400, SRX3400 and SRX3600.
junos-srx5000*	Junos OS for SRX 5600 and SRX5800.

Junos OS Package Names

You upgrade the Juniper Networks Junos operating system (Junos OS) on a Juniper Networks EX Series Ethernet Switch by copying a software package to your switch or another system on your local network, then install the new software package on the switch.

Two versions of a Junos OS image-a controlled version that supports Media Access Control Security (MACsec) and a domestic version that does not support MACsec-are available for EX Series switches. A domestic version of Junos OS is available for all EX Series switches; a controlled version of Junos OS is only available for EX Series switches on Junos OS releases that support MACsec. The domestic version of Junos OS on EX Series switches can be used on any switch in any geography. The controlled version of Junos OS contains encryption and is not available to customers in all geographies.

NOTE: **The controlled version of Junos OS contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS is also subject to controls imposed under the laws of other countries.**

If you have questions about acquiring the controlled version of Junos OS in your country, contact the Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

NOTE: The domestic version of Junos OS on EX Series switches is intended for use on any switch in any worldwide location.

For most Junos packages on other Juniper Networks products, the domestic package is used for products installed in the United States and Canada only while an export package is used for products installed in any worldwide location.

domestic-signed indicates the domestic software package.

A domestic software package name is in the following format:

***package-name-m.nZx.y*-domestic-signed.tgz**

A controlled software package name is in the following format:

***package-name-m.nZx.y*-controlled-signed.tgz**

where:

- ***package-name*** is the name of the package—for example, **jinstall-ex-4200**.
- ***m.n*** is the software release, with ***m*** representing the major release number and *n* representing the minor release number—for example, **9.5**.
- ***Z*** indicates the type of software release, where **R** indicates released software and **B** indicates beta-level software.
- ***x.y*** represents the version of the major software release (*x*) and an internal tracking number (*y*)—for example, **1.6**.
- **domestic-signed** indicates the domestic software package.
- **controlled-signed** indicates the controlled software package.

A sample EX Series software domestic package name is:

```
jinstall-ex-4200-9.5R1.6-domestic-signed.tgz
```

A sample EX Series controlled package name is:

```
jinstall-ex-4200-13.2X50-D15.3-controlled-signed.tgz
```

Related Documentation

- Installing Software on EX Series Switches (J-Web Procedure) on page 64
- Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure) on page 52
- Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure) on page 59
- Downloading Software Packages from Juniper Networks on page 42
- Understanding Software Installation on EX Series Switches on page 35

Software Naming Convention

All Junos OS conforms to the following naming convention:

package-release-edition-cfxxx-signed.*comp*

For example:

jinstall-9.2R1.8–domestic-signed.tgz

where:

- ***package*** is the name of the Junos OS package. For 64-bit Junos OS, the package name is ***package64***.
- ***cfxxx*** designates the CompactFlash card size to use with the software. This value is optional.
- **signed** means that the software includes a digital signature for verification purposes. This value is not used with all software packages.

Software Naming Convention (SRX Series and J Series Devices)

Typically, you upgrade your device software by downloading a software image to your device from another system on your local network. Using the J-Web user interface or the CLI to upgrade, the device downloads the software image, decompresses the image, and installs the decompressed software. Finally, you reboot the device, at which time it boots from the upgraded software. Junos OS is delivered in signed packages that contain digital signatures to ensure official Juniper Networks software.

Software Naming Convention for SRX Series Devices

An upgrade software package name for an SRX Series device is in the following format:

package-name-m.nZx-distribution.tgz

- **package-name**—Name of the package; for example, junos-srxsme.
- **m.n**—Junos OS release, with m representing the major release number and n representing the minor release number; for example, 10.0.
- **Z**—Type of Junos OS release; for example, R indicates released software, and B indicates beta-level software.
- **x.y**—Junos OS build number and spin number; for example, 1.8.
- **distribution**—Area for which the Junos OS package is provided. It is domestic for the United States and Canada, and it is export for worldwide distribution.

The following package name is an example of an SRX Series device upgrade Junos OS package:

junos-srxsme-10.0R1.8-domestic-tgz

Software Naming Convention for J Series Routers

An upgrade software package name for a J Series device is in the following format:

package-name-m.nZx-distribution.tgz.

- **package-name**—Name of the package; for example, junos-jsr.
- **m.n** —Junos OS release, with m representing the major release number and n representing the minor release number; for example, 8.5.
- **Z**—Type of Junos OS release. For example, R indicates released software, and B indicates beta-level software.
- **x.y**—Junos OS build number and spin number; for example, 1.1.
- **distribution**—Area for which the Junos OS package is provided. It is domestic for the United States and Canada, and it is export for worldwide distribution.

The following package name is an example of a Junos OS upgrade package:

junos-jsr-8.5R1.1-domestic.tgz.

Junos OS Recovery Packages

Download a Junos OS recovery package, also known as an install media package, to recover a primary CompactFlash (CF) card.

The Junos OS recovery package recovery package name for a J Series device is in the following format:

package-name-m.nZx-export-cfnnn.gz.

- **package-name**—Name of the package; for example, junos-jsr.
- **m.n** —Junos OS release, with m representing the major release number; for example, 8.5.
- **Z**—Type of Junos OS release. For example, R indicates released software, and B indicates beta-level software
- **x.y**—Junos OS build number and spin number; for example, 1.1.
- **export**—Export indicates that the Junos OS recovery package is the exported worldwide software package version.
- **cfnnn**—Size of the target CF card in megabytes; for example, cf256. The following CF card sizes are supported:
  - 512 MB
  - 1024 MB

NOTE: **The CF cards with less than 512 MB of storage capacity are not supported**

The following example is of a Junos OS recovery package name:

junos-jsr-8.5R1.1-export-cf256.gz

Related Documentation

- Understanding Junos OS Upgrades for J Series and SRX Series Devices on page 188
- *Preparing the USB Flash Drive and Upgrading the Boot Loader for SRX Series Devices*
- Downloading Junos OS Upgrade Packages on J Series and SRX Series Devices on page 193
- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- Installing Junos OS Upgrade Packages on J Series and SRX Devices from a Remote Server on page 193
- *Installation and Upgrade Guide*

Software Package Information Security

All Junos OS is delivered in signed packages that contain digital signatures, Secure Hash Algorithm (SHA-1), and Message Digest 5 (MD5) checksums. A package is installed only if the checksum within it matches the hash recorded in its corresponding file. Which checksum is used depends on the software version:

- Digital signatures are used when you upgrade or downgrade between Junos OS Release 7.0 and a later version.
- The SHA-1 checksum is used when you upgrade or downgrade between Junos OS Release 6.4 and a later version.
- The MD5 checksum is used when you upgrade or downgrade between Junos OS Release 6.3 or earlier and a later version.

Junos OS Release Numbers

The Junos OS release number represents a particular revision of the software that runs on a Juniper Networks routing platform, for example, Junos OS Release 8.5, 9.1, or 9.2. Each Junos OS release has certain new features that complement the software processes that support Internet routing protocols, control the device's interfaces and the device chassis itself, and allow device system management. On the Juniper Networks Support Web page, you download Junos OS for a particular Junos OS release number.

The following example shows how the software release number is formatted:

m.nZb.s

For example:

9.2R1.8

Where:

- *m* is the major release number of the product
- *n* is the minor release number of the product
- *Z* is the type of software release. The following release types are used:
  - *R*—FRS/Maintenance release software
  - *B*—Beta release software
  - *I*—Internal release software: Private software release for verifying fixes
  - *S*—Service release software: Released to customers to solve a specific problem—this release will be maintained along with the life span of the underlying release
  - *X*—Special (eXception) release software: Released to customers to solve an immediate problem—customers are expected to migrate to a supported release when available
- *b* is the build number of the product
  - if *b=1*: Software is the FRS release
  - if *b>1*: Software is a maintenance release
- *s* is the spin number of the product

Related Documentation

- Junos OS Installation Packages on page 5

Installation Media

The installation media is used to recover a device from a software failure. The installation media repartitions the media and completely reinstalls Junos OS. No information from previous installations is retained during this installation. Thus, an initial configuration is required before the device can be put back into service. For more information about creating an initial configuration, see the *Getting Started Guide* for your device.

NOTE: **Once you have rebuilt a device using the installation media, access to the device is restricted to the console port until the management port is configured during the initial configuration.**

The following installation media files are available for download:

Installation Media	Description
floppy1–<*release*>* **floppy2–<*release*>***	Junos OS for the M40 router when you use the LS-120 external drive.
install-media*	Junos OS for the ACX Series, M Series, MX Series, T Series, PTX Series Packet Transport Routers, TX Matrix, and TX Matrix Plus routers.

junos-jsr-<*release*>-export-cf<*size*>.gz	Junos OS for the J Series routers. You must select the correct installation media file that corresponds to the correct CompactFlash card you are using.

NOTE: Branch SRX Series Services Gateways are upgraded from loader prompt using USB or TFTP. For more details, see "Installing Junos OS on SRX Series Devices (Using Boot Loader and USB)" on page 66.

Installation Bundles

The installation bundle can be used to downgrade or upgrade Junos OS between minor revisions (from Release 9.1 to Release 9.2, for example). When used, the installation bundle modifies only the files required for the upgrade or downgrade between versions.

NOTE: You should only use the installation bundle under direction of a Juniper Networks support representative.

The following installation bundle files are available for download:

Installation Bundle	Description
jbundle*	Junos OS for the ACX series, M Series, MX Series, T Series, PTX Series Packet Transport Routers, TX Matrix, and TX Matrix Plus routers.

Installation Modules

Installation modules are used to upgrade individual software modules in Junos OS. For example, you can upgrade only the Routing Engine software by installing the **jroute*** installation module.

NOTE: You should only use installation module files under the direction of a Juniper Networks support representative.

The following installation module files are available for download:

Installation Module	Description
jkernel*	The kernel and network tools package. This package contains the basic operating system files.
jbase*	The base package for Junos OS. This package contains additions to the operating system.

jroute*	The Routing Engine package. This package contains the Routing Engine software.
jpfe*	The Packet Forwarding Engine package. This package contains the PFE software.
jdocs*	The documentation package. This package contains the documentation set for the software.
jcrypto*	The encryption package. This package contains the domestic version of the security software.
jweb*	The J-Web package. This package contains the graphical user interface software for M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and J Series routers.

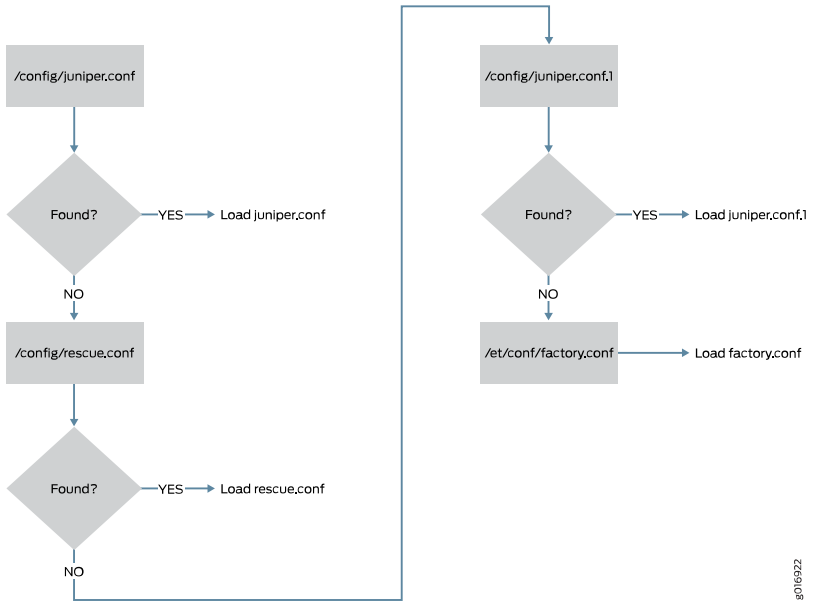
Configuration Files

All configuration settings for the device are handled in the configuration files on the device. These files are saved in the **/config** directory on the device.

Configuration File Selection Sequence

During the boot process, the device is configured based on a predefined configuration file. The device selects the configuration file based on the sequence shown in Figure 1 on page 14.

Figure 1: Configuration Selection Sequence



1. **/config/juniper.conf**—Active configuration file.
2. **/config/rescue.conf**—Rescue configuration file. This file is created by the router or switch administrator.
3. **/config/juniper.conf.1**—First rollback configuration.
4. **/etc/config/factory.conf**—Default factory configuration file.

   The **factory.conf** file is the initial device configuration file shipped with the system. All configuration settings are returned to the factory default, and access to the device is restricted to the console. For more information about setting up your device from the factory default configuration, see the specific hardware guide for your device.

For SRX Series Services Gateways running Junos Release 10.0 or later, the current operational Junos Software configuration is stored in a file named **juniper.conf**, and the last five committed configurations are stored in the files **juniper.conf.1** through **juniper.conf.5**. The rescue configuration is stored in a file named **rescue.conf**. These files are located in the **/config directory** available on the flash drive of the SRX Series Services Gateway.

To list the configuration files, use the **file list /config** operational mode command.

```
user@host>file list / config
/config:
.snap/
idp-dfa-status.db
juniper.conf+.gz
juniper.conf.1.gz
juniper.conf.2.gz
juniper.conf.3.gz
juniper.conf.4.gz
```

```
juniper.conf.5.gz
juniper.conf.gz
juniper.conf.md5*
jwxd_initialized
license/
license-status.db
rescue.conf.gz
usage.db
usage.db.1344499761
```

Remote Storage of Configuration Files

Configuration files can be stored off the device. This can be helpful if the device encounters a software failure or other problem that forces you to restore the device's software. Once the software is restored, you can then reload the saved configuration file. For more information about restoring Junos OS, see "Load and Commit the Configuration File" on page 247.

When the configuration file is stored off the device, you can encrypt the configuration files using the Data Encryption Standard (DES) encryption algorithm.

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 15
- Junos OS Processes on page 16

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.
- Routing Engine—Provides three main functions:
  - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network

- Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
- Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

Junos OS Processes

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

Table 3 on page 16 describes the primary Junos OS processes.

Table 3: Junos OS Processes

Process	Name	Description
Chassis process	chassisd	Detects hardware on the system that is used to configure network interfaces. Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered. Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.
Ethernet switching process	eswd	Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces. Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.
Forwarding process	pfem	Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.
Interface process	dcd	Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.
Management process	mgd	Provides communication between the other processes and an interface to the configuration database. Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured. Interacts with the other processes when commands are issued through one of the user interfaces on the switch. If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.

Table 3: Junos OS Processes *(continued)*

Process	Name	Description
Routing protocol process	rpd	Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.

Related Documentation

- For more information about processes, see *Junos OS Network Operations Guide*
- For more information about basic system parameters, supported protocols, and software processes, see *Junos OS System Basics Configuration Guide*

CHAPTER 2

Hardware Overview

Hardware Architecture Overview

Juniper Network routing platforms are made up of two basic routing components:

- Routing Engine—The Routing Engine controls the routing updates and system management.
- Packet Forwarding Engine (PFE)—The Packet Forwarding Engine performs Layer 2 and Layer 3 packet switching, route lookups, and packet forwarding.

From a system administration perspective, you install the software onto the Routing Engine and during the installation, the appropriate software is forwarded to other components as necessary. Most Routing Engines include a CompactFlash card that stores Junos OS. On M Series Multiservice Edge Routers, MX240, MX480, and MX960 3D Universal Edge Routers, T Series Core Routers, and TX Matrix routers, the system also includes a hard disk or solid-state drive (SSD) that acts as a backup boot drive. PTX Series Packet Transport Routers and the TX Matrix Plus router include a solid state drive as a backup boot drive.

NOTE: The MX80 router is a single-board router with a built-in Routing Engine and single Packet Forwarding Engine. On an MX80 router, Junos OS is stored on dual, internal NAND flash devices. These devices provide the same functionality as a CompactFlash card and hard disk or solid-state drive (SSD).

NOTE: The ACX Series router is a single board router with a built-in Routing Engine and one Packet Forwarding Engine. The ACX router supports dual-root partitioning, which means that the primary and backup Junos OS images are kept in two independently bootable root partitions. If the primary partition becomes corrupted, the system remains fully functional by booting from the backup Junos OS image located in the other root partition.

On routing platforms with dual Routing Engines, each Routing Engine is independent with regard to upgrading the software. To install new software on both Routing Engines, you need to install the new software on each Routing Engine. On platforms with dual Routing Engines configured for high availability, you can use the unified in-service software upgrade procedure to upgrade the software. For more information about this procedure, see the *High Availability Feature Guide for Routing Devices*.

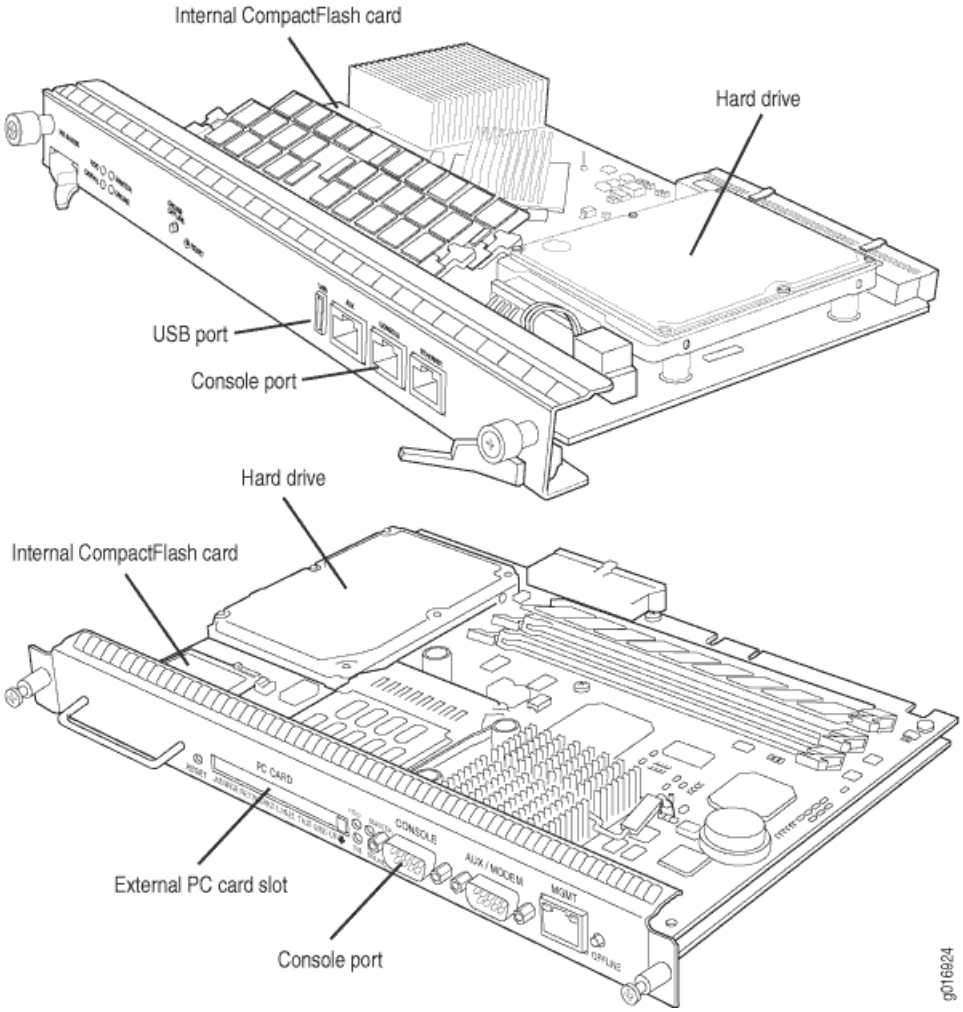
Related Documentation

- *Dual-Root Partitioning ACX Series Universal Access Routers Overview*

Hardware Overview (ACX Series, M Series, MX Series, T Series, and TX Matrix Routers)

Figure 2 on page 21 shows examples of Routing Engines.

Figure 2: Routing Engines



The ACX Series, M Series, MX Series, PTX Series, T Series, TX Matrix, and TX Matrix Plus routers include the following:

- System Memory on page 21
- Storage Media on page 22

System Memory

Starting with Junos OS Release 9.0, all routing platforms require a minimum of 512 MB of system memory on each Routing Engine. All M7i and M10i routers delivered before December 7, 2007, had 256 MB of memory. These routers require a system memory upgrade before you install Junos OS Release 9.0 or a later release. To determine the amount of memory currently installed on your system, use the **show chassis routing-engine** command in the command-line interface (CLI).

For more information about upgrading your M7i or M10i router, see the Customer Support Center JTAC Technical Bulletin PSN-2007-10-001: https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2007-10-001&actionBtn=Search.

ACX2000 routers are shipped with 2 GB of memory and ACX1000 routers with 1 GB of memory.

Storage Media

Except for the ACX Series, MX80 routers, MX104 routers, the M Series, MX Series, PTX Series, T Series, TX Matrix, and TX Matrix Plus routers use the following media storage devices:

- CompactFlash card—The CompactFlash card is typically the primary storage device for most routers.

  NOTE: **M7i and M10i routers using RE-400 are not delivered from the factory with the CompactFlash card installed. In this case, the hard disk is the primary and only boot device. The M7i and M10i routers with RE-400 can be upgraded to include the CompactFlash card.**

- Hard disk or solid -state drive—For most routers,, a hard disk or solid-state drive is the secondary boot device. When the CompactFlash card is not installed on the router, the hard disk or the solid-state drive becomes the primary boot device. The hard disk or solid-state drive is also used to store system log files and diagnostic dump files.
- Emergency boot device—Depending on the router, the emergency boot device can be a PC card, a USB storage device, or an LS-120 floppy disk.

On MX80 routers, the internal NAND flash devices (first *da0*, then *da1*) act as the primary and secondary boot devices.

On ACX Series routers, the internal NAND flash devices (first da0s1, then da0s2) act as the primary and secondary boot devices.

Emergency boot devices can be used to revive a routing platform that has a damaged Junos OS. When an emergency boot device is attached to the router, the router attempts to boot from that device before it boots from the CompactFlash card, solid-state drive (SSD), or hard disk.

On an ACX Series router, the emergency boot device is a USB storage device.

On MX104 routers, the internal NAND flash device (**da0**) mounted on the internal eUSB card acts as the primary boot and storage device. On MX104 routers, the emergency boot device is a USB storage device that is plugged into one of the USB ports in the front plate.

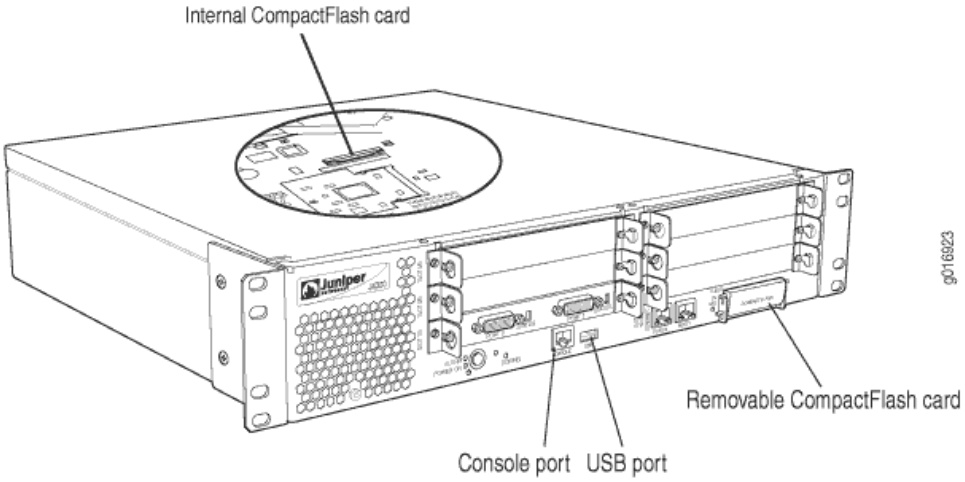
When booting from an emergency boot device, the router requests a boot acknowledgment on the console interface. If you enter yes, the emergency boot device repartitions the primary boot device and reloads Junos OS onto the primary boot device. After the loading is complete, the routing platform requests that you remove the

emergency boot device and reboot the system. After the reboot is complete, you must perform an initial configuration of the router before it can be used on your network.

Hardware Overview (J Series Routers)

The Junos OS is installed on the internal CompactFlash card. This internal CompactFlash card is the primary and only boot drive on the J Series routers when they are delivered from the factory. All J Series routers have one or more USB ports. The 4300 and 6300 J Series routers also include an external CompactFlash card slot. You can install external storage devices through the USB ports and CompactFlash card slots. When external storage devices are installed, these external devices can be used as backup boot drives. You can also create a backup internal boot drive on any externally attached CompactFlash card. This CompactFlash card can then be used to replace the internal CompactFlash card on the J Series router in the event that the internal card is damaged or otherwise made unusable by the router. Figure 3 on page 23 shows the location of the memory and ports on a J Series router.

Figure 3: J Series Routers (J4300 Shown)



The J Series routers include the following:

- System Memory on page 23
- Storage Media on page 24

System Memory

Starting with Junos OS Release 9.1, all J Series routers require a minimum of 512 MB of router memory on each Routing Engine. Any router without this minimum requires a system memory upgrade before you install Junos OS Release 9.1. To determine the amount of memory currently installed on your router, use the CLI **show chassis routing-engine** command.

For more information about memory requirements for the J Series routers, see the Customer Support Center JTAC Technical Bulletin PSN-2008-04-021: http://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2008-04-021&actionBtn=Search.

Storage Media

The J Series routers use the following media storage devices:

- Internal CompactFlash card—The CompactFlash card is the primary boot device.
- External media device—Depending on the system, this external device can be a CompactFlash card or a USB storage device. Juniper Networks recommends that you attach an external device to the system and use this external device as the backup boot device for the system.

Table 4 on page 24 specifies the storage media names used by the J Series routers. The storage media device names are displayed as the router boots.

Table 4: Routing Engines and Storage Media Names (J Series Routers)

Routing Engine	Internal CompactFlash Card	External CompactFlash Card J4300 and J6300 Routers Only	USB Storage Media Devices
J Series Routers	**ad0**	**ad2**	**da0**

To view the storage media currently available on your system, use the CLI **show system storage** command. For more information about this command, see the *CLI User Guide*.

The router attempts to boot from the storage media in the following order:

1. Internal CompactFlash card
2. External CompactFlash card (J4300 and J6300 routers only)
3. USB storage media device

Related Documentation

- Boot Sequence on J Series Routers and SRX Series Devices on page 30
- *Installation and Upgrade Guide*

Hardware Overview (SRX Series Services Gateway)

SRX Series Device Hardware Overview

Figure 4 on page 24 shows example of SRX240 device.

Figure 4: SRX240 Device Front Panel

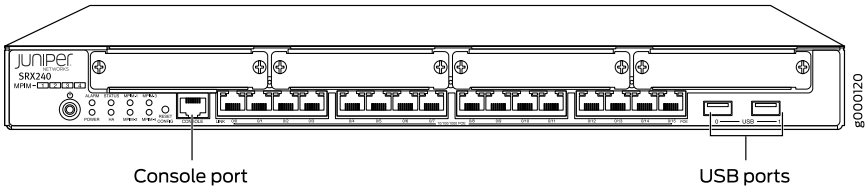


Figure 5 on page 25 shows example of SRX650 device.

Figure 5: SRX650 Device System Routing Engine

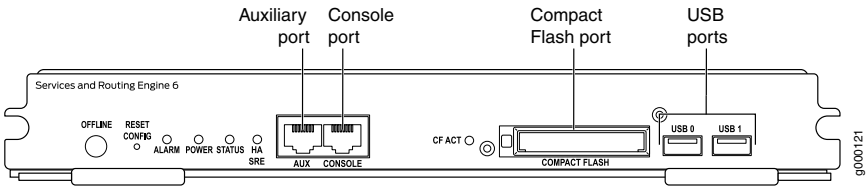
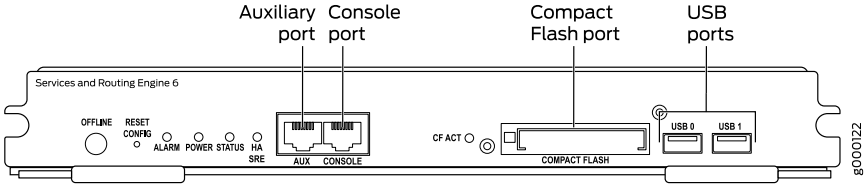


Figure 6 on page 25 shows an example of SRX5800 device Routing Engine.

Figure 6: SRX5800 Device Routing Engine



System Memory

The amount of free disk space necessary to upgrade a device with a new version of the Junos OS can vary from one release to another for different SRX Series devices. Check the Junos OS software version you are installing to determine the free disk space requirements.

To determine the amount of free disk space on the device, issue the **show system storage detail** command. The command output displays statistics about the amount of free disk space in the device file systems.

Storage Media

The SRX100, SRX210, SRX240, Services Gateway can boot from the following storage media (in the order of priority):

- Internal NAND Flash (default; always present)
- USB storage key (alternate)

The SRX550 and SRX650 Services Gateway can boot from the following storage media (in the order of priority):

- CompactFlash (default; always present)
- External CompactFlash card (alternate) (SRX650 only)
- USB storage key (alternate)

SRX1400, SRX3400, SRX3600, SRX5600, SRX5800 devices use the following media storage devices:

- The CompactFlash card in the Routing Engine

- The hard disk in the Routing Engine

NOTE: You can also use a Junos OS image stored on a USB flash drive that you insert into the Routing Engine faceplate.

Related Documentation

- Boot Sequence on J Series Routers and SRX Series Devices on page 30
- *Installation and Upgrade Guide*

Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, PTX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers)

Table 5 on page 26 specifies the storage media names by Routing Engine. The storage media device names are displayed when the router boots.

Table 5: Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers)

Routing Engine	CompactFlash Card	Hard Disk	Solid State Drive	Removable Media Emergency Boot Device
RE-400-768 (RE5)	ad0	ad1	No	ad3
RE-600-2048 (RE3)	ad0	ad1	No	ad3
RE-850-1536 (RE-850)	ad0	ad1	No	ad3
RE-A-1000-2048 (RE-A-1000)	ad0	ad2	No	da0
RE-A-1800x2 (RE-A-1800)	ad0	No	Yes SSD1: ad1 SSD2: ad2	da0
RE-S-1300-2048 (RE-S-1300)	ad0	ad2	No	da0
RE-S-1800x2 RE-S-1800x4 (RE-S-1800)	ad0	No	Yes SSD1: ad1 SSD2: ad2	da0
RE-B-1800X1-4G-S	ad0	No	Yes SSD1: ad1	da0

Table 5: Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers) *(continued)*

Routing Engine	CompactFlash Card	Hard Disk	Solid State Drive	Removable Media Emergency Boot Device
RE-1600-2048 (RE4)	ad0	ad1	No	ad3 and ad4
RE-A-2000-4096 (RE-A-2000)	ad0	ad2	No	da0
RE-S-2000-4096 (RE-S-2000)	ad0	ad2	No	da0
RE-MX-104	No	da0	No	da1 and da2
RE-DUO-C2600-16G (RE-DUO-2600)	ad0	No	ad1	da0
RE-DUO-C1800-8G- (RE-DUO-1800)	ad0	No	ad1	da0
RE-DUO-C1800-16G	ad0	No	ad1	da0
RE-JCS1200-1x2330	da0	da1	No	da2

NOTE: On MX80 routers, the Routing Engine is a built-in device and has no model number. The dual internal NAND flash devices are *da0* and *da1*. The USB storage device is *da2*.

NOTE: On ACX Series routers, the Routing Engine is a built-in device, which does not have a model number. The dual internal NAND flash devices are da0s1 and da0s2. The USB storage device is da0s2a. Use the **show chassis hardware models** command to obtain the field-replaceable unit (FRU) model number—for example, **ACX2000BASE-DC** for the ACX2000 router.

To view the storage media currently available on your system, use the CLI **show system storage** command. For more information about this command, see the *CLI User Guide*.

Related Documentation

- *Supported Routing Engines by Router*
- *Routing Engine Specifications*
- *RE-S-1300 Routing Engine Description*
- *RE-S-2000 Routing Engine Description*

- *RE-S-1800 Routing Engine Description for MX Series*
- *JCS1200 Routing Engine Description*

Routing Engines and Storage Media Names (J Series Routers)

Table 4 on page 24 specifies the storage media names used by the J Series routers. The storage media device names are displayed as the router boots.

Table 6: Routing Engines and Storage Media Names (J Series Routers)

Routing Engine	Internal CompactFlash Card	External CompactFlash Card J4300 and J6300 Routers Only	USB Storage Media Devices
J Series Routers	ad0	ad2	da0
SRX Series device	da0	NA	da1

To view the storage media currently available on your system, use the CLI **show system storage** command. For more information about this command, see the *CLI User Guide*.

Boot Sequence on M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series Devices with Routing Engines

NOTE: **For information about which Routing Engines are supported by each device, see** http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/general/routing-engine-m-mx-t-series-support-by-chassis.html.

The M Series, MX Series (except for the MX80 routers and the MX104 routers), T Series, and TX Matrix routers with a Routing Engine that has a hard disk attempt to boot from the storage media in the following order:

1. Removable media emergency boot device, such as a PC Card (if present)
2. CompactFlash card (if present)
3. Hard disk

The M Series and MX Series with a Routing Engine that has a solid-state drive (SSD) attempt to boot from the storage media in the following order:

1. USB media emergency boot device (if present)
2. CompactFlash card
3. Solid-state drive (SSD) in the SSD slot 1 or SSD slot 2 (if present)

MX80 routers attempt to boot from the storage media in the following order:

1. USB media emergency boot device
2. Dual, internal NAND flash device (first *da0*, then *da1*)

MX104 routers attempt to boot from the storage media in the following order:

1. USB storage media device
2. Internal NAND flash device (**da0**)

The T series routers with a Routing Engine that has a solid-state drive (SSD), and TX Matrix Plus routers attempt to boot from the storage media in the following order:

1. USB media emergency boot device
2. CompactFlash card (if present)
3. Solid-state drive (SSD) in the Disk 1 slot (if present)

   NOTE: **The Disk 2 slot is not currently supported.**

4. Storage media available on the LAN

The ACX Series routers attempt to boot from the storage media in the following order:

1. USB storage media device
2. Dual, internal NAND flash device (first **da0s1**, then **da0s2**)

The PTX Series Packet Transport Routers attempt to boot from the storage media in the following order:

1. USB media emergency boot device
2. CompactFlash card
3. Solid-state drive (SSD) in the Disk 1 slot (if present)
4. Storage media available on the LAN

NOTE: **Do not insert an emergency boot device during normal operations. The router does not operate normally when it is booted from an emergency boot device.**

If the router boots from an alternate boot device, Junos OS displays a message indicating this when you log in to the router. For example, the following message shows that the software booted from the hard disk (**/dev/ad1s1a**):

login: *username*
Password: *password*
Last login: date on *terminal*

```
--- Junos 8.0 R1 built date
---
--- NOTICE: System is running on alternate media device (/dev/ad2s1a).
```

This situation results when the router detects a problem with the primary boot device—usually the CompactFlash card—that prevents it from booting, and consequently boots from the alternate boot device (the hard disk drive). When this happens, the primary boot device is removed from the list of candidate boot devices. The problem is usually a serious hardware error. We recommend you contact the Juniper Networks Technical Assistance Center (JTAC).

NOTE: On MX104 routers, if the router boots from an alternate boot device, Junos OS does not display any message indicating this when you log in to the router.

When the router boots from the alternate boot device, the software and configuration are only as current as the most recent **request system snapshot** command. However, if the **mirror-flash-on-disk** command was enabled, then the hard disk drive contains a synchronized, mirror image of the compact flash drive and therefore the current software and configuration.

Related Documentation

- *Routing Engine Specifications*

Boot Sequence on J Series Routers and SRX Series Devices

The J Series routers attempt to boot from the storage media in the following order:

1. Internal CompactFlash card
2. External CompactFlash card (J4300 and J6300 routers only)
3. USB storage media device

On SRX Series devices, the device attempts to boot from the storage media in the following order:

- Internal CompactFlash card
- USB storage media device

Related Documentation

- Hardware Overview (SRX Series Services Gateway) on page 24
- *Installation and Upgrade Guide*

PART 2

Installing Junos Software

CHAPTER 3

Installation Overview

Installation Type Overview

The three types of installations used to upgrade or downgrade your routing platform are standard installation, category change installation, and recovery installation. The standard installation is the standard method of upgrading and downgrading the software. Use a category change installation when you are moving from one software category to another; for example, if you are changing the device from using the standard Junos OS to the Junos-FIPS category. Perform a recovery installation when the software on the device is damaged or otherwise unable to accommodate a software upgrade or downgrade.

Standard Installation

A standard installation is the typical method used to upgrade or downgrade software on the server. This method uses the installation package that matches the installation package already installed on the system. For example, you might upgrade an M120 router running Junos OS installed using the **jinstall*** installation package. If you upgrade the router from Release 9.0R2.10 to Release 9.1R1.8, you use the **jinstall-9.1R1.8–domestic-signed.tgz** installation package. For information on the different installation packages available, see "Junos OS Installation Packages" on page 5.

Category Change Installation

The category change installation process is used to move from one category of Junos OS to another on the same router; for example, moving from a Junos OS standard installation on an M Series, MX Series, or T Series router to a Junos-FIPS installation. When moving from one installation category to another, you need to be aware of the restrictions regarding this change.

NOTE: Juniper Networks does not support using the **request system software rollback** command to restore a different installation category on the device. When installing a different Junos OS category on a device, once the installation is complete, you should execute a **request system snapshot** command to delete the backup installation from the system.

Recovery Installation

A recovery installation is performed to repair a device with damaged software or a condition that prevents the upgrade, downgrade, or change in installation category of the software.

For example, you may need to perform a recovery installation to change a device's software category from Junos-FIPS to standard Junos OS.

Installation Categories on the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus Routers

The following installation categories are available with the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers:

- Standard Junos OS, domestic—**jinstall-<release>-domestic-signed.tgz**

  This software includes high-encryption capabilities for data leaving the router. Because of U.S. government export restrictions, this software can only be installed on systems within the United States and Canada. For all other customers, a valid encryption agreement is required to use this software edition. Furthermore, no router can be shipped out of the United States. or Canada without the domestic edition first being overwritten by the export edition. There are no current system-enforced restrictions when you install this software category.

- Standard Junos OS, export—**jinstall-<release>-export-signed.tgz**

  This software does not include high-encryption capabilities. It can be installed on any system worldwide. There are no current system-enforced restrictions when you install this software category.

- Junos-FIPS—**junos-juniper-<release>-domestic-signed.tgz** and **junos-juniper-<release>-fips-signed.tgz**

  The Junos-FIPS OS base provides customers with the software tools to configure the router for use within a Federal Information Processing Standards (FIPS) environment. Once you have installed this software category onto a router, you cannot install a different software category on the router using the **request system software add** command. When attempting to install a different Junos OS category package on the router, you receive the following warning message:

  WARNING: Package jinstall-*<release>-<edition>*-signed is not compatible with this system.
  WARNING: Please install a supported package (junos-juniper-*.tgz).

To return to a standard Junos OS category installation, you must perform a system recovery installation of the software. All configuration files, logs, and other data files on the server are overwritten during a recovery installation.

For more information about Junos-FIPS OS base, see "FIPS 140-2 Security Compliance" on page 5.

NOTE: When you install a Junos OS installation package, the previous installation is maintained as a backup installation. You should issue a **request system software snapshot** command to overwrite the backup files any time you change software categories on a router. This is mandatory if the router is to be shipped outside of the United States or Canada after the Export edition of Junos OS has been installed. There are no current system-enforced restrictions when you install this software category,

Installation Categories on the J Series and SRX Series Devices

The following installation categories are available with the SRX Series devices and J Series routers:

- Junos OS, domestic—**junos-srxsme-<release>-domestic.tgz** for SRX Series devices and **junos-jsr-<release>-domestic.tgz** for J Series Routers.

  This software includes high-encryption capabilities for data leaving the router. Because of U.S. government export restrictions, this software can only be installed on systems within the United States and Canada. For all other customers, a valid encryption agreement is required to use this software edition. Furthermore, no router can be shipped out of the United States. or Canada without the domestic edition first being overwritten by the export edition. There are no current system-enforced restrictions when you install this software category.

- Junos OS, export—**junos-srxsme-<release>-export.tgz** for SRX Series devices and **junos-jsr-<release>-export.tgz** for J Series Routers.

This software does not include high-encryption capabilities. It can be installed on any system worldwide. There are no current system-enforced restrictions when you install this software category.

Understanding Software Installation on EX Series Switches

A Juniper Networks EX Series Ethernet Switch is delivered with the Juniper Networks Junos operating system (Junos OS) preinstalled. As new features and software fixes become available, you must upgrade your software to use them. You can also downgrade Junos OS to a previous release.

This topic covers:

Overview of the Software Installation Process

An EX Series switch is delivered with a domestic version of Junos OS preinstalled. When you connect power to the switch, it starts (boots) from the installed software.

You upgrade Junos OS on an EX Series switch by copying a software package to your switch or another system on your local network, then use either the J-Web interface or the command-line interface (CLI) to install the new software package on the switch. Finally, you reboot the switch; it boots from the upgraded software. After a successful upgrade, you should back up the new current configuration to a secondary device. You should following this procedure regardless of whether you are installing a domestic or controlled Junos OS package.

During a successful upgrade, the upgrade package removes all files from **/var/tmp** and completely reinstalls the existing software. It retains configuration files, and similar information, such as secure shell and host keys, from the previous version. The previous software package is preserved in a separate disk partition, and you can manually revert back to it if necessary. If the software installation fails for any reason, such as loss of power during the installation process, the system returns to the originally active installation when you reboot.

Software Package Security

All Junos OS releases are delivered in signed packages that contain digital signatures to ensure official Juniper Networks software. For more information about signed software packages, see the *Junos OS Installation and Upgrade Guide*.

Installing Software on a Virtual Chassis

You can connect individual EX Series switches together to form one unit and manage the unit as a single device, called a Virtual Chassis. The Virtual Chassis operates as a single network entity composed of member switches. Each member switch in a Virtual Chassis must be running the same version of Junos OS. See *EX Series Virtual Chassis Software Features Overview* for a list of switches that can be used in a Virtual Chassis.

For ease of management, a Virtual Chassis provides flexible methods to upgrade software releases. You can deploy a new software release to all member switches of a Virtual Chassis or to only a particular member switch

You can also upgrade the software on an EX4200, EX4500, mixed EX4200 and EX4500, and EX8200 Virtual Chassis using nonstop software upgrade (NSSU). NSSU takes advantage of graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) to ensure no disruption to the control plane during the upgrade. You can minimize

disruption to network traffic by defining link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards (on EX8200 Virtual Chassis) or on different members (on EX4200, EX4500, mixed EX4200 and EX4500 Virtual Chassis). During an NSSU, the line cards and Virtual Chassis members are upgraded one at a time, so that traffic continues to flow through the other line cards or members while that line card or member is being upgraded.

Installing Software on Switches with Redundant Routing Engines

You can install software on a switch with redundant Routing Engines in one of two ways:

- Perform an NSSU—An NSSU upgrades both Routing Engines with a single command and with a minimum of network disruption. An NSSU takes advantage of GRES and NSR to ensure no disruption to the control plane. You can minimize disruption to network traffic by defining LAGs such that the member links of each LAG reside on different line cards. The line cards are upgraded one at a time, so that traffic continues to flow through the other line cards while a line card is being upgraded.

  You cannot use NSSU to downgrade the software running on a switch.

  For more information about NSSU, see "Understanding Nonstop Software Upgrade on EX Series Switches" on page 121. See *EX Series Switch Software Features Overview* for a list of switches that support NSSU.

- Upgrade each Routing Engine manually—You can perform a Junos OS installation on each Routing Engine separately, starting with the backup Routing Engine. You can use this procedure to downgrade the software running on a switch. See "Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)" on page 59.

Installing Software Using Automatic Software Download

The automatic software download feature uses the DHCP message exchange process to download and install software packages. Users can define a path to a software package on the DHCP server and then the DHCP server communicates this path to EX Series switches acting as DHCP clients as part of the DHCP message exchange process. The DHCP clients that have been configured for automatic software download receive these messages and, when the software package name in the DHCP server message is different from that of the software package that booted the DHCP client switch, download and install the software package. See "Upgrading Software by Using Automatic Software Download" on page 178.

Autoinstalling a Configuration File on an EX2200 or EX3300 Switch from a Disk-on-Key USB Memory Stick

You can use an autoinstallation process to configure the software on an EX2200 or EX3300 switch. You can use a configuration file that is in either text format or XML format. If you want to use an XML-formatted file, you use a Junos Space platform to create the configuration file. You place the configuration file on a Disk-on-Key USB memory stick. See *Autoinstalling a Configuration File from a Disk-on-Key USB Memory Stick onto an EX2200 or EX3300 Switch*.

Troubleshooting Software Installation

If Junos OS loads but the CLI is not working for any reason, or if the switch has no software installed, you can use the recovery installation procedure to install the software on the switch. See "Troubleshooting Software Installation" on page 321.

NOTE: You can also use this procedure to load two versions of Junos OS in separate partitions on the switch.

Related Documentation

- Downloading Software Packages from Juniper Networks on page 42
- Installing Software on EX Series Switches (J-Web Procedure) on page 64
- Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure) on page 52
- Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure) on page 59
- Understanding Nonstop Software Upgrade on EX Series Switches on page 121

CHAPTER 4

Performing a Standard or Change Category Installation

Checking the Current Configuration and Candidate Software Compatibility

When you upgrade or downgrade Junos OS, we recommend that you include the **validate** option with the **request system software add** command to check that the candidate software is compatible with the current configuration. By default, when you add a package with a different release number, the validation check is done automatically.

NOTE: On an ACX Series router, you must ensure that the primary and backup partitions are synchronized after an upgrade by issuing the **request system snapshot** command.

Related Documentation

- request system software add on page 373
- request system snapshot on page 365

Determining the Junos OS Version

To determine which software packages are running on the device and to get information about these packages, use the **show version** operational mode command at the top level of the command-line interface (CLI).

NOTE: The **show version** command does not show the software category installed, only the release number of the software.

Downloading Software

You can download the software in one of two ways:

- Downloading Software with a Browser on page 40
- Downloading Software Using the Command-Line Interface on page 41

Downloading Software with a Browser

You download the software package you need from the Juniper Networks Support Web site at http://www.juniper.net/support/.

NOTE: To access the download section, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks Web site: https://www.juniper.net/registration/Register.jsp.

To download the software:

1. In a browser, go to http://www.juniper.net/support/.

   The Support page opens.

2. In the Download Software section, select the software version to download.

   Depending on your location, select Junos Canada and US, or Junos Worldwide.

3. Select the current release to download.
4. Click the Software tab and select the Junos OS Installation Package to download.

A dialog box opens.

5. Save the file to your system. If you are placing the file on a remote system, you must make sure that the file can be accessible by the router or switch using HTTP, FTP, or scp.

Downloading Software Using the Command-Line Interface

Download the software package you need from the Juniper Networks Support Web site at http://www.juniper.net/support/, and place the package on a local system. You can then transfer the downloaded package to the device using either the router or switch command-line interface, or the local system command-line interface.

NOTE: **To access the download section, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks Web site:** https://www.juniper.net/registration/Register.jsp.

Before you transfer the software package, ensure that the FTP service is enabled on the device.
Enable the FTP service using the **set system services ftp** command:

```
user@host# set system services ftp
```

To transfer the software package using the device command-line interface:

1. From the router or switch command line, initiate an FTP session with the local system (host) where the package is located using the **ftp** command:

   ```
   user@host> ftp host
   ```

   host is the Hostname or address of the local system.

2. Log in with your customer support–supplied username and password:

   ```
   User Name: username
   331 Password required for username.
   Password: password
   ```

   Once your credentials have been validated, the FTP session opens.

3. Navigate to the software package location on the local system, and transfer the package using the **get** command:

   ```
   user@host> get installation-package
   ```

   Following is an example of an *installation-package* name:
   jinstall-9.2R1.8–domestic-signed.tgz

4. Close the FTP session using the **bye** command:

   ```
   user@host> bye
   Goodbye
   ```

To transfer the package using the local system command-line interface:

1. From the local system command line, initiate an FTP session with the device using the **ftp** command:

   user@host> **ftp** ***host***

   host is the Hostname or address of the router or switch.

2. Log in with your customer support–supplied username and password:

   User Name: ***username***
   331 Password required for username.
   Password: ***password***

   Once your credentials have been validated, the FTP session opens.

3. Navigate to the software package location on the local system, and transfer the package using the **put** command:

   user@host> **put** ***installation-package***

   Following is an example of an *installation-package* name:
   jinstall-9.2R1.8–domestic-signed.tgz

4. Close the FTP session using the **bye** command:

   user@host> **bye**
   Goodbye

Downloading Software Packages from Juniper Networks

You can download Junos OS packages from the Juniper Networks website to upgrade software on your EX Series switch.

Before you begin to download software upgrades, ensure that you have a Juniper Networks Web account and a valid support contract. To obtain an account, complete the registration form at the Juniper Networks website: https://www.juniper.net/registration/Register.jsp.

To download software upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. For EX Series, there are not separate software packages for Canada the U.S. and other locations. Therefore, select **Canada and U.S. Version** regardless of your location:

   - https://www.juniper.net/support/downloads/junos.html

2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Using the J-Web interface or the CLI, select the appropriate software package for your application. See "Junos OS Package Names" on page 6.

4. Download the software to a local host or to an internal software distribution site.

Related Documentation

- Installing Software on EX Series Switches (J-Web Procedure) on page 64
- Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure) on page 52
- Understanding Software Installation on EX Series Switches on page 35

Understanding Download Manager for SRX Series Devices

Overview

This download manager feature facilitates download of large files over low-bandwidth links. It enables you to download large Junos OS packages over low-bandwidth/flaky links so that the system can be upgraded. This feature allows you to download multiple files while monitoring their status and progress individually. It takes automatic action when required and displays status information when requested.

This feature is supported on SRX100, SRX210, SRX220, SRX240, and SRX650 Services Gateways.

This feature provides the following functions:

- Bandwidth-limited downloads
- Scheduled downloads
- Automatic resume on error
- Automatic resume on reboot

NOTE: **This feature supports only the FTP and HTTP protocols.**

Using Download Manager to Upgrade Junos OS

The download manager acts as a substitute for the FTP utility. You can use the download manager CLI commands for all the functions where you previously used the FTP utility.

The download manager requires the following:

- FTP or HTTP server with a Junos OS image
- Server that is reachable from the device being upgraded

The download manager consists of the following CLI commands:

1. To download the Junos OS image to your device, use the **request system download start** command (set a bandwidth limit, if required). The file is saved to the **/var/tmp** directory on your device.

   You can continue to use the device while the download runs in the background.

2. Use the **show system download** command to verify that the file has been downloaded. The command displays the state as "completed" when the downloaded file is ready to be installed.

3. Use the **request system software add** command to install the downloaded image file from the **/var/tmp** directory.

Handling Errors

If you encounter any problem with a download, use the **show system download <id>** command to obtain details about the download.

Table 7 on page 44 lists the output fields for the **show system download** command. Use this information to diagnose problems. Output fields are listed in the approximate order in which they appear.

Table 7: show system download Output Fields

Output Field	Description
Status	State of the download.
Creation Time	Time the **start** command was issued.
Scheduled Time	Time the download was scheduled to start.
Start Time	Time the download actually started (if it has already started).
Retry Time	Time for next retry (if the download is in the error state).
Error Count	Number of times an error was encountered by this download.
Retries Left	Number of times the system will retry the download automatically before stopping.
Most Recent Error	Message indicating the cause of the most recent error.

Considerations

- When no download limit is specified for a specific download or for all downloads, a download uses all available network bandwidth.
- Because the download limit that you set indicates an average bandwidth limit, it is possible that certain bursts might exceed the specified limit.

- When a download from an HTTP server fails, the server returns an HTML page. Occasionally, the error page is not recognized as an error page and is downloaded in place of the Junos image file.
- Remote server logins and passwords are stored by the download manager for the duration of a download. To encrypt these credentials provided along with the login keyword, define an encryption key with the **request system set-encryption-key** command. Any changes to encryption settings while download is in progress can cause the download to fail.
- A download command issued on a particular node in a chassis cluster takes place only on that node and is not propagated to the other nodes in the cluster. Downloads on different nodes are completely independent of each other. In the event of a failover, a download continues only if the server remains reachable from the node from which the command was issued. If the server is no longer reachable on that node, the download stops and returns an error.

Related Documentation

- *Junos OS CLI Reference*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

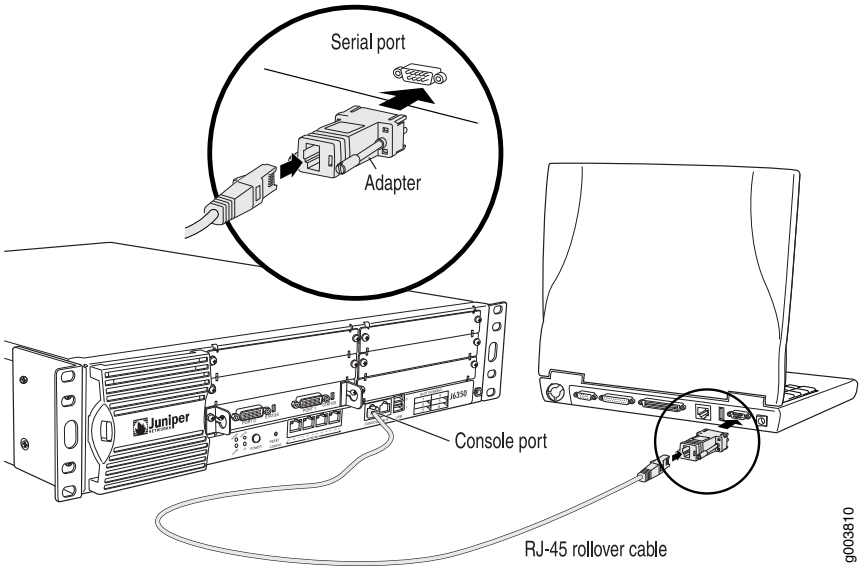
Understanding the Console Port

Console ports allow root access to the Junos operating system (Junos OS) devices through a terminal or laptop interface, regardless of the state of the Junos OS device, unless it is completely powered off. By connecting to the console port, you can access the root level of the Junos OS device without using the network to which the device might or might not be connected. This creates a secondary path to the Junos OS device without relying on the network.

Using the terminal interface provides a technician sitting in a Network Operations Center a long distance away the ability to restore a Junos OS device or perform an initialization configuration securely, using a modem, even if the primary network has failed. Without a connection to the console port, a technician would have to visit the site to perform repairs or initialization. A remote connection to the Junos OS device through a modem requires the cable and connector (provided in the device accessory box), plus a DB-9 male to DB-25 male (or similar) adapter for your modem, which you must purchase separately. For more information about connecting to the console port, see the administration guide for your particular router or switch.

To configure the device initially, you must connect a terminal or laptop computer to the device through the console port, as shown in Figure 7 on page 46.

Figure 7: Connecting to the Console Port on a Junos OS Device



Related Documentation

- *Accessing a Junos OS Device the First Time*

Backing Up the Current Installation (ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus Routers)

You should back up the current installation so that you can return to the current software installation. In a dual Routing Engine system, you need to back up both Routing Engines. This section covers the following:

The installation process using the installation package (**jinstall***, for example) removes all stored files on the router except the **juniper.conf** and SSH files. Therefore, you should back up your current configuration in case you need to return to the current software installation after running the installation program.

To back up Junos OS on the M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers, issue the **request system snapshot** CLI operational command. This command saves the current software installation on the hard disk or solid-state drive (SSD).

NOTE: On M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus router with dual Routing Engines, complete this operation on both Routing Engines. On routers without a CompactFlash card, where the hard disk is the primary boot device, you cannot back up your software installation. On MX104 routers, which do not have a CompactFlash card, you can back up your software installation on an external USB storage media device.

When the **request system snapshot** command is issued, the **/root** file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The **/root** and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are

on the router's hard disk or or solid-state drive (SSD). When the backup is completed, the current and backup software installations are identical.

To copy the files to the router's hard disk or solid-state drive (SSD), use the following command:

```
user@host> request system snapshot
```

On MX104 routers, when you issue the **request system snapshot** operational command to back up the current software installation, the backup is taken on the first USB storage media device. You can also specify the USB storage media device on which the back up must be taken by using these commands:

```
user@host > request system snapshot media usb0
user@host > request system snapshot media usb1
```

To back up Junos OS on the ACX Series routers, issue the **request system snapshot slice alternate** CLI operational command. When this command is issued, the **/root** file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig** file systems on the router's NAND flash device.

To copy the files to the router's NAND flash device, use the following command:

```
user@host> request system snapshot slice alternate
```

To copy the files from the NAND flash device to a USB storage media device, use the following command:

```
user@host> request system snapshot
```

Related Documentation

- request system snapshot on page 365
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

Backing Up the Current Installation on J Series and SRX Series Devices

This topic includes the following section:

Backing Up the Current Installation on J Series Devices

You should back up the current installation so that you can return to the current software installation. In a dual Routing Engine system, you need to back up both Routing Engines.

The installation process using the installation package (**junos-jsr***) removes all stored files on the router except the **juniper.conf** and SSH files. Therefore, you should back up your current configuration in case you need to return to the current software installation after running the installation program.

The following instructions offer the minimum steps required to create a backup on a J Series router during the installation process. For a complete description of the backup process on the J Series routers, see the *Junos OS Administration Guide for Security Devices* and the *Junos OS Systems Basics Configuration Guide*.

To back up Junos OS on the J Series routers:

1. Attach an external memory device to the router.

   NOTE: Even when attached to a J Series router, the USB memory device is not listed as a storage device in the **show system storage** CLI command output. You can view the installed USB memory device on the J-Web interface's system monitor screen.

2. Issue the **request system snapshot media usb** command.

   The current software installation and configuration are saved on the external USB storage device.

Backing Up the Current Installation on SRX Series Devices

On SRX Series devices, you can backup the current Junos OS image and configuration files onto a media (such as a USB or CompactFlash) so that you can retrieve it back if something goes wrong.

Following procedure shows how to backup current installation on an SRX650 device.

The SRX650 Services Gateway includes the following 2 GB CompactFlash (CF) storage device:

- The Services and Routing Engine (SRE) contains a hot-pluggable external CF storage device used to upload and download files.
- The chassis contains an internal CF used to store the operating system.

By default, only the internal CF is enabled and an option to take a snapshot of the configuration from the internal CF to the external CF is not supported. This can be done only by using a USB storage device.

To take a snapshot of the configuration from the external CF:

1. Take a snapshot from the internal CF to a USB storage device using the **request system snapshot media usb** command.
2. Reboot the device from the USB storage device using the **request system reboot media usb** command.
3. Go to the U-boot prompt.
4. Stop at U-boot and set the following variables:

```
set ext.cf.pref 1
   save
   reset
```

5. Once the system is booted from the USB storage device, take a snapshot from the external CF using the **request system snapshot media external** command.

NOTE: Once the snapshot is taken on the external CF, we recommend that you set the ext.cf.pref to 0 at the U-boot prompt.

Configuring External CompactFlash on SRX650 Devices

The SRX650 Services Gateway includes the following 2 GB CompactFlash (CF) storage device:

- The Services and Routing Engine (SRE) contains a hot-pluggable external CF storage device used to upload and download files.
- The chassis contains an internal CF used to store the operating system.

By default, only the internal CF is enabled and an option to take a snapshot of the configuration from the internal CF to the external CF is not supported. This can be done only by using a USB storage device.

To take a snapshot of the configuration from the external CF:

1. Take a snapshot from the internal CF to a USB storage device using the **request system snapshot media usb** command.
2. Reboot the device from the USB storage device using the **request system reboot media usb** command.
3. Go to the U-boot prompt.
4. Stop at U-boot and set the following variables:

```
set ext.cf.pref 1
   save
   reset
```

5. Once the system is booted from the USB storage device, take a snapshot from the external CF using the **request system snapshot media external** command.

NOTE: Once the snapshot is taken on the external CF, we recommend that you set the ext.cf.pref to 0 at the U-boot prompt.

Related Documentation

- Understanding Junos OS Upgrades for J Series and SRX Series Devices on page 188
- Configuring Boot Devices for J Series and SRX Series Devices on page 216
- Installing Junos OS on SRX Series Devices (Using Boot Loader and USB) on page 66
- *Installation and Upgrade Guide*

Installing the Software Package on a Router with a Single Routing Engine

To upgrade the router or switch software, follow these steps:

1. Install the new software package using the **request system software add** command:

   user@host> **request system software add /var/tmp/*installation-package***

   installation-package is the name of the installation package; for example **jinstall-9.2R1.8–domestic-signed.tgz**

   For M Series, MX Series, and T Series routers and Branch SRX Series firewall filters running Junos OS Release 12.2 and above, you can use the **request system software add set** command to install multiple software packages at one time:

   user@host> **request system software add set /var/tmp/*installation-package***

   installation-package can either be a list of installation packages, each separated by a blank space, or the full URL to the directory or tar file containing the list of installation packages.

   WARNING: Do not include the *re0 | re1* option when you install a package using the **request system software add** command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package are the same. In such cases, the package gets deleted after a successful upgrade.

   For more information about the **request system software add** command, see the CLI Explorer.

2. Reboot the device to start the new software using the **request system reboot** command:

   user@host> **request system reboot**
   Reboot the system? [yes, no] (no) **yes**

   NOTE: You must reboot the device to load the new installation of Junos OS on the device.

   To abort the installation, do not reboot the device. Instead, finish the installation and then issue the **request system software delete jinstall** command. This is your last chance to stop the installation.

   The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The device then reboots from the boot device on which the software was just installed. When the reboot is complete, the device displays the login prompt.

   While the software is being upgraded, the Routing Engine on which you are performing the installation does not route traffic.

3. Log in and issue the **show version** command to verify the version of the software installed.

4. (Optional) Add the **jweb** package using the **request system software add** command. Before you can add this package, you must first download the software as you did the installation package. For more information about downloading the **jweb** package, see "Downloading Software" on page 40.

   The **jweb** installation module adds a device management graphical user interface that you can use to view and configure your device. For more information about the **jweb** package, see "Installation Modules" on page 12.

5. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the **request system snapshot** command to back up the new software.

Related Documentation

- Repartitioning Routing Engine System Storage To Increase the Swap Partition on page 64

Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)

You can use this procedure to upgrade Junos OS on a single routing engine in any EX Series switch, including all switches that do not support redundant Routing Engines. You can also use this procedure to upgrade software on all EX Series Virtual Chassis, with the exception of the EX8200 Virtual Chassis.

This procedure can be used to upgrade the following switches or Virtual Chassis:

- EX2200 switch
- EX3200 switch
- EX3300 switch
- EX4200 switch
- EX4300 switch
- EX4500 switch
- EX4550 switch
- EX6200 switch (single Routing Engine upgrade only)
- EX8200 switch (single Routing Engine upgrade only)
- All Virtual Chassis except EX8200 Virtual Chassis

To upgrade software on an EX6200 or EX8200 switch running two Routing Engines, see "Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)" on page 59 or "Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)" on page 132.

To upgrade software on an EX8200 Virtual Chassis, see *Installing Software for All Devices in an EX8200 Virtual Chassis*.

To install software upgrades on a switch with a single Routing Engine:

1. Download the software package as described in "Downloading Software Packages from Juniper Networks" on page 42.
2. (Optional) Back up the current software configuration to a second storage option. See the *Junos OS Installation and Upgrade Guide* for instructions on performing this task.
3. (Optional) Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.

   This step is optional because Junos OS can also be upgraded when the software image is stored at a remote location. These instructions describe the software upgrade process for both scenarios.
4. Install the new package on the switch:

   user@switch> **request system software add *package***

   Replace ***package*** with one of the following paths:

- For a software package in a local directory on the switch—**/var/tmp/*package*.tgz**.
- For a software package on a remote server:
  - **ftp://*hostname/pathname/package*.tgz**
  - **http://*hostname/pathname/package*.tgz**

where *package*.tgz is, for example, **jinstall-ex-4200-9.4R1.8-domestic-signed.tgz**.

Include the optional **member** option to install the software package on only one member of an EX4200 Virtual Chassis:

user@switch> request system software add ***source*** member ***member-id*** reboot

Other members of the Virtual Chassis are not affected. To install the software on all members of the Virtual Chassis, do not include the **member** option.

NOTE: To abort the installation, do not reboot your device; instead, finish the installation and then issue the **request system software delete** *package*.tgz command, where *package*.tgz is, for example, **jinstall-ex-4200-10.2R1.8-domestic-signed.tgz**. This is your last chance to stop the installation.

5. Reboot to start the new software:

   user@switch> request system reboot

6. After the reboot has completed, log in and verify that the new version of the software is properly installed:

   user@switch> **show version**

7. To ensure that the resilient dual-root partitions feature operates correctly, execute the following command to copy the new Junos OS image into the alternate root partition:

   user@switch> request system snapshot **slice alternate**

   To update the alternate root partitions on all members of a Virtual Chassis, use this command:

   user@switch> **request system snapshot slice alternate all-members**

   Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Related Documentation

- Installing Software on EX Series Switches (J-Web Procedure) on page 64
- Troubleshooting Software Installation on page 321
- Junos OS Package Names on page 6
- Understanding Software Installation on EX Series Switches on page 35

Installing the Software Package on a Router with Redundant Routing Engines

If the router has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

WARNING: **If graceful Routing Engine switchover (GRES), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI delete chassis redundancy command when prompted. If GRES is enabled, it will be removed with the redundancy command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the [edit routing-options] hierarchy level to disable it.**

To upgrade the router software, perform the following tasks:

1. Preparing the Router for the Installation on page 54
2. Installing Software on the Backup Routing Engine on page 55
3. Installing Software on the Master Routing Engine on page 56
4. Finalizing the Installation on page 58

Preparing the Router for the Installation

Perform the following steps before installing the software:

1. Log in to the master Routing Engine's console.

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your router.

2. From the router command line, enter configuration mode:

   a.
   ```
   user@host#> configure
   Entering configuration mode

   [edit]
   user@host#
   ```

3. Disable Routing Engine redundancy:

   ```
   [edit]
   user@host# delete chassis redundancy
   ```

4. Save the configuration change on both Routing Engines:

   ```
   [edit]
   user@host# commit synchronize
   ```

5. Exit out of the CLI configuration mode:

   ```
   [edit]
   user@host# exit
   ```

Installing Software on the Backup Routing Engine

After the router has been prepared, you first install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine and then upgrade or downgrade the software version on the other Routing Engine.

1. Log in to the console port on the other Routing Engine (currently the master).

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your router.

2. Install the new software package using the **request system software add** command:

   user@host> **request system software add validate /var/tmp/jinstall-9.2R1.8–domestic-signed.tgz**

   For M Series, MX Series, and T Series routers and Branch SRX Series firewall filters running Junos OS Release 12.2 and above, you can use the **request system software add set** command to install multiple software packages at the same time:

   user@host> **request system software add set /var/tmp/*installation-package***

   installation-package can either be a list of installation packages, each separated by a blank space, or the full URL to the directory or tar file containing the list of installation packages.

   Use the **request system software add set** command to retain any SDK configuration by installing the SDK add-on packages along with the core Junos OS installation package.

   WARNING: Do not include the ***re0 | re1*** option when you install a package using the **request system software add** command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package are the same. In such cases, the package gets deleted after a successful upgrade.

   For more information about the **request system software add** command, see the CLI Explorer.

3. Reboot the router to start the new software using the **request system reboot** command:

   user@host> **request system reboot**
   Reboot the system? [yes, no] (no) **yes**

NOTE: You must reboot the device to load the new installation of Junos OS on the router.

To abort the installation, do not reboot your device. Instead, finish the installation and then issue the **request system software delete jinstall** command. This is your last chance to stop the installation.

All the software is loaded when you reboot the device. Installation can take between 5 and 10 minutes. The router then reboots from the boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation is not routing traffic.

4. Log in and issue the **show version** command to verify the version of the software installed.

5. (Optional) Add the **jweb** package using the **request system software add** command. Before you can add this package, you must first download the software as you did the installation package. For more information about downloading the **jweb** package, see "Downloading Software" on page 40.

   The **jweb** installation module adds a router management graphical user interface that you can use to view and configure your router. For more information about the **jweb** package, see "Installation Modules" on page 12.

Installing Software on the Master Routing Engine

Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine and then upgrade or downgrade the master Routing Engine software:

1. Log in to the master Routing Engine console port.

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your router.

2. Transfer routing control to the backup Routing Engine:

   ```
   user@host> request chassis routing-engine master switch
   ```

   For more information about the **request chassis routing-engine master** command, see the CLI Explorer.

3. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

   ```
   user@host> show chassis routing-engine
   Routing Engine status:
    Slot 0:
     Current state          Backup
     Election priority       Master (default)
   Routing Engine status:
    Slot 1:
     Current state          Master
   ```

Election priority Backup (default)

4. Install the new software package using the **request system software add** command:

```
user@host> request system software add validate
/var/tmp/jinstall-9.2R1.8–domestic-signed.tgz
```

For M Series, MX Series, and T Series routers and Branch SRX Series firewall filters running Junos OS Release 12.2 and above, you can use the **request system software add set** command to install multiple software packages at the same time:

```
user@host> request system software add set /var/tmp/installation-package
```

installation-package can either be a list of installation packages, each separated by a blank space, or the full URL to the directory or tar file containing the list of installation packages.

Use the **request system software add set** command to retain any SDK configuration by installing the SDK add-on packages along with the core Junos OS installation package.

WARNING: Do not include the *re0* | *re1* option when you install a package using the **request system software add** command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package are the same. In such cases, the package gets deleted after a successful upgrade.

For more information about the **request system software add** command, see the CLI Explorer.

5. Reboot the Routing Engine using the **request system reboot** command:

```
user@host> request system reboot
Reboot the system? [yes, no] (no) yes
```

NOTE: You must reboot to load the new installation of Junos OS on the router.

To abort the installation, do not reboot your system. Instead, finish the installation and then issue the **request system software delete jinstall** command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The router then reboots from the boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not route traffic.

6. Log in and issue the **show version** command to verify the version of the software installed.

7. (Optional) Add the **jweb** package using the **request system software add** command. Before you can add this package, you must first download the software as you did the installation package. For more information about downloading the **jweb** package, see "Downloading Software" on page 40.

   The **jweb** installation module adds a router management graphical user interface that you can use to view and configure your router. For more information about the **jweb** package, see "Installation Modules" on page 12.

8. Transfer routing control back to the master Routing Engine:

   ```
   user@host> request chassis routing-engine master switch
   ```

   For more information about the **request chassis routing-engine master** command, see the CLI Explorer.

9. Verify the master Routing Engine (slot 0) is indeed the master Routing Engine:

   ```
   user@host> show chassis routing-engine
   Routing Engine status:
    Slot 0:
      Current state          Master
      Election priority       Master (default)
   outing Engine status:
    Slot 1:
      Current state          Backup
      Election priority       Backup (default)
   ```

Finalizing the Installation

Once the software is installed on both Routing Engines, you return the router back to its original configuration and back up the new installation.

1. Restore the configuration that existed before you deleted it at the start of this procedure:

   ```
   {backup}
     user@host-re0> configure
     [edit]
   user@host-re0# rollback 1
   ```

2. Save the configuration change on both Routing Engines:

   ```
   [edit]
   user@host-re0> commit synchronize and-quit
   ```

3. After you have installed the new software and are satisfied that it is successfully running, issue the **request system snapshot** command to back up the new software on both master and backup Routing Engines:

   ```
   {master}
     user@host-re0> request system snapshot
     {master}
     user@host-re0> request routing-engine login other routing-engine
     {backup}
     user@host-re1> request system snapshot
   {backup}
   ```

The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router's hard disk or solid-state drive (SSD).

For more information about the **request routing-engine login** command, see the CLI Explorer.

NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running copy and backup copy of the software are identical.

Related Documentation

- Repartitioning Routing Engine System Storage To Increase the Swap Partition on page 64

Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)

For an EX6200 switch or an EX8200 switch with redundant Routing Engines, you can minimize disruption to network operation during a Junos OS upgrade by upgrading the Routing Engines separately, starting with the backup Routing Engine.

NOTE: If your EX8200 switch is running Junos OS Release 10.4R3 or later, you can upgrade the software packages on both Routing Engines with a single command and with minimal network disruption by using nonstop software upgrade (NSSU) instead of this procedure. See "Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)" on page 132.

WARNING: If graceful routing engine switchover (GRES) or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you disable GRES before you begin the software installation by using the **deactivate chassis redundancy graceful-switchover** command in configuration mode. If GRES is enabled, it will be removed with the redundancy command. By default, NSR is disabled. If NSR is enabled, remove the **nonstop-routing** statement from the **[edit routing-options]** hierarchy level to disable it.

To upgrade the software package on an EX6200 switch or an EX8200 switch with one installed Routing Engine, see "Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)" on page 52.

To upgrade redundant Routing Engines, you first install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master

Routing Engine. After making sure that the new software version is running correctly on the backup Routing Engine, you switch device control to the backup Routing Engine. Finally, you install the new software on the new backup Routing Engine.

To upgrade Junos OS on the switch, perform the following tasks:

1. Preparing the Switch for the Software Installation on page 60
2. Installing Software on the Backup Routing Engine on page 61
3. Installing Software on the Default Master Routing Engine on page 62
4. Returning Routing Control to the Default Master Routing Engine (Optional) on page 63

Preparing the Switch for the Software Installation

Perform the following steps before installing the software:

1. Log in to the master Routing Engine's console.

   For information on logging in to the Routing Engine through the console port, see *Connecting and Configuring an EX Series Switch (CLI Procedure)*.

2. Enter the Junos OS CLI configuration mode:

   a. Start the CLI from the shell prompt:

      user@switch:RE% **cli**

      You will see:

      {master}
      user@switch>

   b. Enter configuration mode:

      user@switch> **configure**

      You will see:

      {master}[edit]
      user@switch#

3. Disable nonstop active routing (NSR) (supported on switches running Junos OS Release 10.4 or later):

   ```
   {master}[edit]
   user@switch#  delete routing-options nonstop-routing
   ```

4. Disable graceful Routing Engine switchover (GRES):

   {master}[edit]
   user@switch# **deactivate chassis redundancy graceful-switchover**

5. Save the configuration change on both Routing Engines:

   {master}[edit]
   user@switch# **commit synchronize**

NOTE: To ensure the most recent configuration changes are committed before the software upgrade, perform this step even if nonstop active routing and graceful Routing Engine switchover were previously disabled.

6. Exit the CLI configuration mode:

```
[edit]
user@switch# exit
```

7. (Optional) Back up the current software configuration to a second storage option. See the *Junos OS Installation and Upgrade Guide* for instructions on performing this task.

Installing Software on the Backup Routing Engine

After you have prepared the switch for software installation, install the software on the backup Routing Engine. During the installation, the master Routing Engine continues operations, minimizing the disruption to network traffic.

1. Download the software by following the procedures in "Downloading Software Packages from Juniper Networks" on page 42.
2. Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.
3. Log in to the console of the backup Routing Engine.
4. Install the new software package:

```
user@switch> request system software add /var/tmp/package.tgz
```

where *package*.tgz is, for example, **jinstall-ex-8200-10.2R1.8-domestic-signed.tgz**.

NOTE: To abort the installation, do not reboot your device; instead, finish the installation and then issue the **request system software delete** *package*.tgz command, where *package*.tgz is, for example, **jinstall-ex-8200-10.2R1.8-domestic-signed.tgz**. This is your last chance to stop the installation.

5. Reboot to start the new software:

```
user@switch> request system reboot
Reboot the system? [yes, no] (no) yes
```

NOTE: You must reboot the switch to load the new installation of the Junos OS.

6. After the reboot has completed, log in and verify the new version of the software is properly installed:

```
user@switch> show version
```

Installing Software on the Default Master Routing Engine

To transfer control to the backup Routing Engine and then upgrade or downgrade the master Routing Engine software:

1. Log in to the master Routing Engine console port.
2. Transfer control to the backup Routing Engine:

   CAUTION: **Because graceful Routing Engine switchover is disabled, this switchover causes all line cards in the switch to reload. All network traffic passing through these line cards is lost during the line card reloads.**

   ```
   user@switch> request chassis routing-engine master switch
   ```

3. Verify that the default backup Routing Engine (shown as slot 1 in the command output) is now the master Routing Engine:

   ```
   user@switch> show chassis routing-engine
   ```

   You will see:

   ```
   Routing Engine status:
    Slot 0:
     Current state          Backup
     Election priority       Master (default)
   Routing Engine status:
    Slot 1:
     Current state          Master
     Election priority       Backup (default)
   ```

4. Install the new software package:

   ```
   user@switch> request system software add package.tgz
   ```

5. Reboot the Routing Engine:

   ```
   user@switch> request system reboot
   Reboot the system? [yes, no] (no) yes
   ```

   When the reboot completes, the prompt will reappear. Wait for this prompt to reappear before proceeding to the next step.

6. Log in to the default backup Routing Engine (slot 1) through the console port.
7. Re-enable graceful Routing Engine switchover:

   ```
   [edit]
   user@switch# activate chassis redundancy graceful-switchover
   ```

   Re-enabling graceful Routing Engine switchover allows any future Routing Engine switchovers to occur without loss of any network traffic.

8. Re-enable nonstop active routing:

   ```
   [edit]
   user@switch# set routing-options nonstop-routing
   ```

NOTE: Automatic commit synchronization is a requirement for nonstop active routing. If you have not yet enabled it, do so with the **set system commit synchronize** command.

9. Save the configuration change:

```
[edit]
user@switch# commit synchronize
```

10. To ensure that the resilient dual-root partitions feature operates correctly, execute the following command to copy the new Junos OS image into the alternate root partition on each Routing Engine:

```
user@switch> request system snapshot slice alternate routing-engine both
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

If you want to return routing control to the Routing Engine that was the master Routing Engine at the beginning of the procedure (the default master Routing Engine), perform the next task.

Returning Routing Control to the Default Master Routing Engine (Optional)

The switch can maintain normal operations with the Routing Engine in slot 1 acting as the master Routing Engine after the software upgrade, so only perform this task if you want to return routing control to the default master Routing Engine in slot 0.

1. Transfer routing control back to the default master Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

2. Verify that the default master Routing Engine (slot 0) is indeed the master Routing Engine:

```
user@switch> show chassis routing-engine
```

You will see:

```
Routing Engine status:
  Slot 0:
    Current state          Master
    Election priority       Master (default)
Routing Engine status:
  Slot 1:
    Current state          Backup
    Election priority       Backup (default)
```

Related Documentation

- Installing Software on EX Series Switches (J-Web Procedure) on page 64
- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) on page 132
- Troubleshooting Software Installation on page 321
- Junos OS Package Names on page 6

- Understanding Software Installation on EX Series Switches on page 35

Repartitioning Routing Engine System Storage To Increase the Swap Partition

You can increase the size of the swap partition by repartitioning the drive (hard disk or solid-state drive (SSD)) on the Routing Engine. This feature is first available in Junos OS Release 10.4R5, 11.1R3, and 11.2R1; in earlier Junos OS releases, the swap partition is not increased by the methods described here.

This behavior applies only to Routing Engines with more than 2 GB of RAM. The new size of the swap partition depends on the size of the drive and the amount of Routing Engine RAM.

- When the drive is 32 GB or less, the swap partition is limited to 8 GB.
- When the drive is larger than 32 GB, the swap partition matches the size of the Routing Engine RAM.

To repartition the drive, perform one of the following actions:

- During the installation of a Junos OS software package (**jinstall***), issue the **request system reboot media disk** command to boot from the drive instead of issuing the **request system reboot** command. The drive is automatically repartitioned. The **request system reboot media disk** command repartitions the drive only during a software upgrade.
- Manually partition the drive by issuing the **request system partition hard-disk** command, and then reboot the router when the command completes.

CAUTION: Repartitioning the drive re-creates the /config and /var directories in the router file system. Although the contents of /config and /var/db are preserved, the remaining contents of /var are lost. For this reason, we recommend that you back up the /var directory before you repartition the SSD on a router with this configuration.

Related Documentation

- Installing the Software Package on a Router with a Single Routing Engine on page 50
- Installing the Software Package on a Router with Redundant Routing Engines on page 54

Installing Software on EX Series Switches (J-Web Procedure)

You can upgrade software packages on a single fixed-configuration switch, on an individual member of a Virtual Chassis, or for all members of a Virtual Chassis.

You can use the J-Web interface to install software upgrades from a server using FTP or HTTP, or by copying the file to the EX Series switch.

This topic describes:

1. Installing Software Upgrades from a Server on page 65
2. Installing Software Upgrades by Uploading Files on page 65

Installing Software Upgrades from a Server

To install software upgrades from a remote server by using FTP or HTTP:

1. Download the software package as described in "Downloading Software Packages from Juniper Networks" on page 42.
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. In the J-Web interface, select **Maintain** > **Software** > **Install Package**.
4. On the Install Remote page, enter information into the fields described in Table 8 on page 65.
5. Click **Fetch and Install Package**. The software is activated after the switch has rebooted.

Table 8: Install Remote Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name.	Type the full address of the software package location on the FTP or HTTP server—one of the following: ftp://*hostname/pathname/package-name* http://*hostname/pathname/package-name*
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	NOTE: The Reboot check box will be disabled if you enter a J-Web Application package name in the Package Location text box. To enable the Reboot check box, enter a Junos package name in the Package Location text box. If this box is checked, the switching platform will automatically reboot when the upgrade is complete.	Check the box if you want the switching platform to reboot automatically when the upgrade is complete.

Installing Software Upgrades by Uploading Files

To install software upgrades by uploading files:

1. Download the software package.
2. In the J-Web interface, select **Maintain>Software>Upload Package**.

3. On the Upload Package page, enter information into the fields described in Table 9 on page 66.
4. Click **Upload and Install Package**. The software is activated after the switching platform completes the installation procedure.

Table 9: Upload Package Summary

Field	Function	Your Action
File to Upload (required)	Specifies the location of the software package.	Type the location of the software package, or click **Browse** to navigate to the location.
Reboot If Required	Specifies that the switching platform is automatically rebooted when the upgrade is complete.	Select the check box if you want the switching platform to reboot automatically when the upgrade is complete.

Related Documentation

- Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure) on page 52
- Understanding Software Installation on EX Series Switches on page 35
- Troubleshooting Software Installation on page 321

Registering the EX Series Switch with the J-Web Interface

NOTE: **This topic applies only to the J-Web Application package.**

You can register your EX Series switch with the J-Web interface so that you can request technical assistance as and when required. To register an EX Series switch:

1. In the J-Web interface, select **Maintain** > **Customer Support** > **Product Registration**. For an EX8200 Virtual Chassis configuration, select the member from the list.

   Note the serial number that is displayed.
2. Click **Register**. Enter the serial number in the page that is displayed.

Related Documentation

- *EX Series Switch Software Features Overview*

Installing Junos OS on SRX Series Devices (Using Boot Loader and USB)

- Installing Junos OS on SRX Series Devices From the Boot Loader Using a TFTP Server on page 67
- Installing Junos OS on SRX Series Devices From the Boot Loader Using an USB Storage Device on page 69
- Installing Junos OS on SRX Series Devices Using a USB Flash Drive on page 70

Installing Junos OS on SRX Series Devices From the Boot Loader Using a TFTP Server

You can install the Junos OS using the Trivial File Transfer Protocol (TFTP) method. The device is shipped with the Junos OS loaded on the primary boot device. During the Junos OS installation from the loader, the device retrieves the Junos OS package from a TFTP server. The internal media is then formatted, and the Junos OS image is installed.

From the loader installation, you can:

- Install the Junos OS on the device for the first time.
- Recover the system from a file system corruption.

NOTE: **Installation from a TFTP server can only be performed using the first onboard Ethernet interface.**

Installation from the loader-over-TFTP method does not work reliably over slow speeds or large latency networks.

Before you begin, verify that:

- You have access to the TFTP server with the Junos OS package to be installed.
- That the TFTP server supports BOOTP or DHCP. If the TFTP server does not support BOOTP or DHCP, you must set the environment variables before performing the installation from the TFTP server.
- Functional network connectivity exists between the device and the TFTP server over the first onboard Ethernet interface.

To install the Junos OS image on the internal media of the device:

1. To access the U-boot prompt, use the console connection to connect to the device.
2. Reboot the device.

   The following messages appear:

   Clearing DRAM..... done BIST check passed. Net: pic init done (err = 0)octeth0 POST Passed

   After this message appears, you see the following prompt:

   Press SPACE to abort autoboot in 3 seconds
3. Press the space bar to stop the autoboot process.

   The => U-boot prompt appears.
4. From the U-boot prompt, configure the environment variables listed in Table 10 on page 68.

Table 10: Environment Variables Settings

Environment Variables	Description
gatewayip	IP address of the gateway device
ipaddr	IP address of the SRX Series device
netmask	network mask
serverip	IP address of the TFTP server

This example shows you how to configure the environment variables:

```
Clearing DRAM..... done
BIST check passed.
Net: pic init done (err = 0)octeth0
POST Passed
Press SPACE to abort autoboot in 3 seconds
=>
=> setenv ipaddr 10.157.70.170
=> setenv netmask 255.255.255.0
=> setenv gatewayip 10.157.64.1
=> setenv serverip 10.157.60.1
=> saveenv
```

5. Reboot the system using the **reset** command.
6. To access the loader prompt, enter use the console connection to connect to the device.
7. Reboot the device.

   The following message appears:

   Loading /boot/defaults/loader.conf

   After this message appears, you see the following prompt:

   Hit [Enter] to boot immediately, or space bar for command prompt.

8. Press the space bar to access the loader prompt.

   The **loader>** prompt appears. Enter:

   loader> **install tftp://10.77.25.12/junos-srxsme-10.0R2-domestic.tgz**

NOTE: The URL path is relative to the TFTP server's TFTP root directory, where the URL is *tftp://tftp-server-ipaddress/package*.

When this command is executed:

- The Junos OS package is downloaded from the TFTP server.
- The internal media on the system is formatted.
- The Junos OS package is installed on the internal media.

NOTE: **The Installation from the loader-over-TFTP method installs Junos OS on the internal CF on SRX100, SRX210, SRX220, and SRX240 devices, whereas on SRX650 devices, this method can install Junos OS on the internal or external CF card.**

After Junos OS is installed, the device boots from the internal media. Once the system boots up with Junos OS Release 10.0 or later, you should upgrade the U-boot and boot loader immediately.

CAUTION: **When you install Junos OS using the loader-over-TFTP method, the media is formatted. The process attempts to save the current configuration. We recommend that you back up all important information on the device before using this process.**

Installing Junos OS on SRX Series Devices From the Boot Loader Using an USB Storage Device

To install Junos OS Release 10.0 or later from the boot loader using a USB storage device:

1. Format a USB storage device in MS-DOS format.
2. Copy the Junos OS image onto the USB storage device.
3. Plug the USB storage device into the SRX Series device.
4. Stop the device at the loader prompt and issue the following command:

   loader> **install file:///*<image-path-on-usb>***

   An example of a command is as follows:

   loader> **install file:///junos-srxsme-10.0R2-domestic.tgz**

   This formats the internal media and installs the new Junos OS image on the media with dual-root partitioning.
5. Once the system boots up with Junos OS Release 10.0 or later, upgrade the U-boot and boot loader immediately.

Installing Junos OS on SRX Series Devices Using a USB Flash Drive

To install the Junos OS image on an SRX Series device:

1. Insert the USB flash drive into the USB port of the SRX Series device and wait for the LEDs to blink amber, then steadily turn amber, indicating that the SRX Series device detects the Junos OS image.

   If the LEDs do not turn amber, press the Power button or power-cycle the device and wait for the LEDs to steadily turn amber.

2. Press the Reset Config button on the SRX Series device and wait for the LEDs to turn green, indicating that the Junos OS upgrade image has successfully installed.

   If the USB device is plugged in, the Reset Config button always performs as an image upgrade button. Any other functionality of this button is overridden until you remove the USB flash drive.

3. Remove the USB flash drive. The SRX Series device restarts automatically and loads the new Junos OS version.

NOTE: If an installation error occurs, the LEDs turn red, which might indicate that the Junos OS image on the USB flash drive is corrupted. An installation error can also occur if the current configuration on the SRX Series device is not compatible with the new Junos OS version on the USB or if there is not enough space on the SRX Series device to install the image. You must have console access to the SRX Series device to troubleshoot an installation error.

NOTE: You can use the **set system autoinstallation usb disable** command to prevent the automatic installation from the USB device. After using this command, if you insert the USB device into the USB port of the SRX Series device, the installation process does not work.

Related Documentation

- Preparing Your J Series and SRX Series Device for Junos OS Upgrades on page 190
- *Preparing the USB Flash Drive and Upgrading the Boot Loader for SRX Series Devices*
- Backing Up the Current Installation on J Series and SRX Series Devices on page 47
- Configuring Boot Devices for J Series and SRX Series Devices on page 216
- *Installation and Upgrade Guide*

Example: Installing Junos OS on SRX Series Devices Using the Partition Option

This example shows how to install Junos OS Release 10.0 or later with the **partition** option.

Requirements

Before you begin, back up any important data.

Overview

This example formats the internal media and installs the new Junos OS image on the media with dual-root partitioning. Reinstall the Release 10.0 or later image from the CLI using the **request system software add** command with the **partition** option. This copies the image to the device, and then reboots the device for installation. The device boots up with the Release 10.0 or later image installed with the dual-root partitioning scheme. When the **partition** option is used, the format and install process is scheduled to run on the next reboot. Therefore, we recommend that this option be used together with the **reboot** option.

NOTE: The process might take 15 to 20 minutes. The system is not accessible over the network during this time.

WARNING: Using the partition option with the request system software add command erases the existing contents of the media. Only the current configuration is preserved. You should back up any important data before starting the process.

NOTE: Partition install is supported on the default media on SRX100, SRX210, and SRX240 devices (internal NAND flash) and on SRX650 devices (internal CF card).

Partition install is *not* supported on the alternate media on SRX100, SRX210, and SRX240 devices (USB storage key) or on SRX650 devices (external CF card or USB storage key).

In this example, add the software package junos-srxsme-10.0R2-domestic.tgz with the following options:

- **no-copy** option to install the software package but do not save the copies of package files. You should include this option if you do not have enough space on the internal media to perform an upgrade that keeps a copy of the package on the device.
- **no-validate** option to bypass the compatibility check with the current configuration before installation starts.
- **partition** option to format and re-partition the media before installation.
- **reboot** option to reboots the device after installation is completed.

Configuration

CLI Quick Configuration

To quickly install Junos OS Release 10.0 or later with the **partition** option, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>request system software add junos-srxsme-10.0R2-domestic.tgz no-copy
  no-validate partition reboot
```

GUI Step-by-Step Procedure

To install Junos OS Release 10.0 or later with the **partition** option:

1. In the J-Web user interface, select **Maintain>Software>Install Package**.
2. On the Install Package page, specify the FTP or HTTP server, file path, and software package name. Type the full address of the software package location on the FTP (*ftp://hostname/pathname/junos-srxsme-10.0R2-domestic.tgz*) or HTTP server (*http://hostname/pathname/junos-srxsme-10.0R2-domestic.tgz*).

   NOTE: **Specify the username and password, if the server requires one.**

3. Select the **Reboot If Required** check box to set the device to reboot automatically when the upgrade is complete.
4. Select the **Do not save backup** check box to bypass saving the backup copy of the current Junos OS package.
5. Select the **Format and re-partition the media before installation** check box to format the internal media with dual-root partitioning.
6. Click **Fetch and Install Package**. The software is activated after the device reboots.

   This formats the internal media and installs the new Junos OS image on the media with dual-root partitioning.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To install Junos OS Release 10.0 or later with the **partition** option:

1. Upgrade the device to Junos OS Release 10.0 or later using the CLI.
2. After the device reboots, upgrade the boot loader to the latest version. See *Preparing the USB Flash Drive and Upgrading the Boot Loader for SRX Series Devices*.
3. Reinstall the Release 10.0 or later image.

```
user@host>request system software add junos-srxsme-10.0R2-domestic.tgz no-copy
  no-validate partition reboot
Copying package junos-srxsme-10.0R2-domestic.tgz to var/tmp/install
Rebooting ...
```

Results

From configuration mode, confirm your configuration by entering the **show system storage partitions** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

Sample output on a system with single root partitioning:

```
user@host> show system storage partitions
Boot Media: internal (da0)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    898M   /
      s1e    24M    /config
      s1f    61M    /var
```

Sample output on a system with dual-root partitioning:

```
user@host> show system storage partitions
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   altroot
      s2a    293M   /
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the Partitioning Scheme Details on page 74

Verifying the Partitioning Scheme Details

Purpose Verify that the partitioning scheme details on the SRX Series device were configured.

Action From operational mode, enter the **show system storage partitions** command.

Related Documentation

- Dual-Root Partitioning Scheme on SRX Series Devices on page 97
- Reinstalling the Single-Root Partition on SRX Series Devices on page 272
- *Installation and Upgrade Guide*

CHAPTER 5

Configuring Zero Touch Provisioning

Understanding Zero Touch Provisioning

NOTE: To see which platforms support Zero Touch Provisioning, in a browser, go to Feature Explorer. In the **Explore Features** section of the Feature Explorer page, select **All Features**. In the **Features Grouped by Feature Family** box, select Zero Touch Provisioning. You can also type the name of the feature in the **Search for Features** edit box. In previous Junos OS releases on EX Series switches, Zero Touch Provisioning was called EZ Touchless Provisioning.

Zero Touch Provisioning allows you to provision new Juniper Networks switches in your network automatically, without manual intervention. When you physically connect a switch to the network and boot it with a default factory configuration, it attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network. To make sure you have the default factory configuration loaded on the switch, issue the **request system zeroize** command on the switch you want to provision.

The switch uses information that you configure on a Dynamic Host Configuration Protocol (DHCP) server to locate the necessary software image and configuration files on the network. If you do not configure the DHCP server to provide this information, the switch boots with the preinstalled software and default factory configuration.

The Zero Touch Provisioning process will either upgrade or downgrade the Junos OS version. During an downgrade:

- On an EX Series switch, If you downgrade to a software version earlier than Junos OS Release 12.2, in which Zero Touch Provisioning is not supported, the configuration file autoinstall phase of the Zero Touch Provisioning process does not happen.
- On an EX Series switch, to downgrade to a software version that does not support resilient dual-root partitions (Junos OS Release 10.4R2 or earlier), you must perform some manual work on the switch. For more information, see "Understanding Resilient Dual-Root Partitions on Switches" on page 93.

NOTE: On QFX3500 and QFX3600 switches running the original CLI, you cannot use ZTP to upgrade from Junos OS Release 12.2 or later to Junos OS Release 13.2X51-D15 or later.

When you boot a switch with the default factory configuration, the following process happens:

1. If DHCP option 43, suboption 00 (the name of the software image file on the FTP, HTTP, or TFTP server) is configured, the switch compares the version of the provided software image to the version of the software installed on the switch.

   NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

2. If DHCP option 43, suboption 02 (a symbolic link to the software image file on the FTP, HTTP, or TFTP server), the switch compares the version of the provided software image to the version of the software installed on the switch.
   - If the Junos OS versions are different, the switch downloads the software image from the FTP, HTTP, or TFTP server, installs the Junos OS, and reboots using the default factory configuration.
   - If the software versions are the same, the switch does not upgrade the software.
3. If DHCP option 43, suboption 01 (the name of the configuration file on the FTP, TFTP, or HTTP server is configured, the switch compares the version of the provided configuration file to the version of the configuration file on the switch.

   If DHCP option 43 suboption 01 is not specified, the switch uses the default factory configuration.

   If the configuration file version on the FTP, HTTP, or TFTP server is newer than the configuration file on the switch, the configuration file is updated on the switch.

   If both DHCP option 43 suboption 01 and suboption 2 are specified, suboption 01 is processed before suboption 02. The Junos OS is upgraded, and then the configuration file is applied.
4. If DHCP option 43, suboption 03 (the transfer mode setting) is configured, the switch accesses the FTP, HTTP, or TFTP server using the specified transfer mode setting—for example, FTP.

   If DHCP option 43, suboption 03, is not configured, TFTP becomes the transfer mode automatically.
5. If DHCP option 43, suboption 04 (the name of the software image file on the FTP, HTTP, or TFTP server) is configured, the switch compares the version of the provided software image to the version of the software installed on the switch.

NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

6. If DHCP option 150 or option 66 is specified, the IP address of the FTP, HTTP, or TFTP server is configured.

   NOTE: You must configure either option 150 or option 66. If you configure both option 150 and option 66, option 150 takes precedence, and option 66 is ignored. Also, make sure you specify an IP address, not a hostname, because name resolution is not supported.

7. (Optional) If DHCP option 7 is specified, you can configure one or more syslog servers.
8. (Optional) If DHCP option 42 is specified, you can configure one or more NTP servers.
9. (Optional) If DHCP option 12 is specified, you can configure the hostname of the switch.

Related Documentation

- Configuring Zero Touch Provisioning on page 78

Configuring Zero Touch Provisioning

NOTE: To see which platforms support Zero Touch Provisioning, in a browser, go to Feature Explorer. In the **Explore Features** section of the Feature Explorer page, select **All Features**. In the **Features Grouped by Feature Family** box, select Zero Touch Provisioning. You can also type the name of the feature in the **Search for Features** edit box. In previous Junos OS releases on EX Series switches, Zero Touch Provisioning was called EZ Touchless Provisioning. Search for that feature name if you want to know if this feature is supported on EX Series switches.

Zero Touch Provisioning allows you to provision new switches in your network automatically, without manual intervention. When you physically connect a switch to the network and boot it with a default configuration, it attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network.

The switch uses information that you configure on a Dynamic Host Control Protocol (DHCP) server to determine whether to perform these actions and to locate the necessary software image and configuration files on the network. If you do not configure the DHCP server to provide this information, the switch boots with the preinstalled software and default configuration.

NOTE: If you have both DHCP and ZTP enabled, the switch broadcasts a DHCP DISCOVER packet every six minutes. If a DHCP server on the network responds with a DHCP ACK packet with DHCP vendor options set with the necessary values to initiate ZTP, then ZTP proceeds.

To disable broadcasting the DHCP DISCOVER packet every six minutes, without performing the ZTP process, manually delete the **auto-image-upgrade** statement located in the **[edit chassis]** hierarchy. If ZTP completes without errors, the auto-image-upgrade statement is automatically deleted.

NOTE: For detailed information regarding the DHCP and DHCP options, refer to RFC2131 (http://www.ietf.org/rfc/rfc2131.txt) and RFC2132 (www.ietf.org/rfc/rfc2132.txt). Also, this document refers to Internet Systems Consortium (ISC) DHCP version 4.2. For more information regarding this version, refer to http://www.isc.org/software/dhcp/documentation.

Before you begin:

- Ensure that the switch has access to the following network resources:

- The DHCP server provides the location of the software image and configuration files on the network

  Refer to your DHCP server documentation for configuration instructions.

- The File Transfer Protocol (anonymous FTP), Hypertext Transfer Protocol (HTTP), Trivial File Transfer Protocol (TFTP) server on which the software image and configuration files are stored

  NOTE: **Although TFTP is supported, we recommend that you use FTP or HTTP instead, because these transport protocols are more reliable.**

- A Domain Name System (DNS) server to perform reverse DNS lookup
- (Optional) An NTP server to perform time synchronization on the network
- (Optional) A system log (syslog) server to manage system log messages and alerts

- Locate and record the MAC address printed on the switch chassis.

CAUTION: **You cannot commit a configuration while the switch is performing the software update process. If you commit a configuration while the switch is performing the configuration file autoinstallation process, the process stops, and the configuration file is not downloaded from the network.**

To configure Zero Touch Provisioning for a switch:

1. Make sure the switch has the default factory configuration installed.

   Issue the **request system zeroize** command on the switch that you want to provision.

2. Download the software image file and the configuration file to the FTP, HTTP, TFTP, server that the switch will download these files from.

   You can download either one or both of these files.

3. Configure the DHCP server to provide the necessary information to the switch.

   Configure IP address assignment.

   You can configure dynamic or static IP address assignment for the switch's management address. To determine the switch's management MAC address for static IP address mapping, add 1 to the last byte of the switch's MAC address, which you noted before you began this procedure.

4. Define the format of the vendor-specific information for DHCP option 43 in the dhcpd.conf file.

   Here is an example of an ISC DHCP 4.2 server dhcpd.conf file:

```
option space NEW_OP;
  option NEW_OP.image-file-name code 0 = text;
  option NEW_OP.config-file-name code 1 = text;
  option NEW_OP.image-file-type code 2 = text;
```

```
option NEW_OP.transfer-mode code 3 = text;
option NEW_OP.alt-image-file-name code 4 = text;
option NEW_OP-encapsulation code 43 = encapsulate NEW_OP;
```

5. Configure the following DHCP option 43 suboptions:

   - Suboption 00: The name of the software image file to install

     NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

     ```
     option NEW_OP.image-file-name
       "/dist/images/jinstall-ex-4200-13.2R1.1-domestic-signed.tgz";
     ```

   - Suboption 01: The name of the configuration file to install

     ```
     option NEW_OP.config-file-name "/dist/config/jn-switch35.config";
     ```

   - Suboption 02: The symbolic link to the software image file to install

     ```
     option NEW_OP.image-file-type "symlink";
     ```

     NOTE: If you do not specify suboption 2, the Zero Touch Provisioning process handles the software image as a filename, not a symbolic link.

   - Suboption 03: The transfer mode that the switch uses to access the TFTP/FTP/HTTP server

     ```
     option NEW_OP.transfer-mode "ftp";
     ```

     NOTE: If suboption 03 is not configured, TFTP becomes the transfer mode by default.

   - Suboption 04: The name of the software image file to install

     NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

     ```
     option NEW_OP.alt-image-file-name
       "/dist/images/jinstall-ex-4200-13.2R1.1-domestic-signed.tgz";
     ```

6. NOTE: You must configure either option 150 or option 66. If you configure both option 150 and option 66, option 150 takes precedence, and option 66 is ignored. Also, make sure you specify an IP address, not a hostname, because name resolution is not supported.

Configure DHCP option 150 to specify the IP address of the FTP, HTTP, or TFTP server.

option option-150 code 150 "10.100.31.71";

7. Configure DHCP option 66 to specify the IP address of the FTP, HTTP, or TFTP server.

   option tftp-server-name "10.100.31.71";

8. (Optional) Configure DHCP option 7 to specify one or more system log (syslog) servers.

   option log-servers 10.100.31.72;

9. (Optional) Configure DHCP option 42 to specify one or more NTP servers.

   option ntp-servers 10.100.31.73;

10. (Optional) Configure DHCP option 12 to specify the hostname of the switch.

    option hostname "jn-switch35";

The following sample configuration shows the DHCP options you just configured:

```
host jn-switch35 {
  hardware ethernet ac:4b:c8:29:5d:02;
  fixed-address 10.100.31.36;
  option tftp-server-name "10.100.31.71";
  option host-name "jn-switch35";
  option log-servers 10.100.31.72;
  option ntp-servers 10.100.31.73;
  option NEW_OP.image-file-name
    "/dist/images/jinstall-ex-4200-13.2R1.1-domestic-signed.tgz";
  option NEW_OP.transfer-mode "ftp";
  option NEW_OP.config-file-name "/dist/config/jn-switch35.config";
}
```

Based on the DHCP options you just configured, the following statements are appended to the Junos OS configuration file (for example, **jn-switch35.config**):

```
system {
  host-name jn-switch35;
  syslog {
    host 10.100.31.72 {
      any any;
    }
  }
  ntp {
    server 10.100.31.73;
  }
}
```

11. Connect the switch to the network that includes the DHCP server and the FTP, HTTP, or TFTP,server.

12. Boot the switch with the default configuration.

13. Monitor the ZTP process by looking at the following log files.

NOTE: When SLAX (live operating system based on Linux) scripts are issued, the **op-script.log** and **event-script.log** files are produced.

- /var/log/dhcp_logfile
- /var/log/image_load_log
- /var/log/op-script.log
- /var/log/event-script.log

Related Documentation

- Understanding Zero Touch Provisioning on page 75
- *Understanding NTP Time Servers*
- *Op Script Overview*
- *Understanding DHCP Services for Switches*
- Reverting to the Default Factory Configuration by Using the request system zeroize Command on page 248

CHAPTER 6

Configuring Automatic Installation of Configuration Files

Autoinstallation Overview (ACX Series Routers, J Series, and SRX Series Devices)

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over the network. You can use either the J-Web configuration editor or the CLI configuration editor to configure a device for autoinstallation.

NOTE: J-Web configuration does not apply to ACX Series Converged Access Gateway routers.

Autoinstallation provides automatic configuration for a new device that you connect to the network and turn on, or for a device configured for autoinstallation. The autoinstallation process begins anytime a device is powered on and cannot locate a valid configuration file in the CompactFlash (CF) card. Typically, a configuration file is unavailable when a device is powered on for the first time, or if the configuration file is deleted from the CF card. The autoinstallation feature enables you to deploy multiple devices from a central location in the network.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the device.

Autoinstallation takes place automatically when you connect an Ethernet or serial port on a new Juniper Networks device to the network and power on the device. To simplify

the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

This section contains the following topics:

- Supported Autoinstallation Interfaces and Protocols on page 84
- Typical Autoinstallation Process on a New Device on page 84

Supported Autoinstallation Interfaces and Protocols

Before autoinstallation on a device can take place, the device must acquire an IP address. The protocol or protocols you choose for IP address acquisition determine the device interface to connect to the network for autoinstallation. The device detects the connected interface and requests an IP address with a protocol appropriate for the interface. Autoinstallation is supported over an Ethernet LAN interface or a serial LAN or WAN interface. Table 11 on page 84 lists the protocols that the device can use on these interfaces for IP address acquisition.

Table 11: Interfaces and Protocols for IP Address Acquisition During Autoinstallation

Interface and Encapsulation Type	Protocol for Autoinstallation
Ethernet LAN interface with High-Level Data Link Control (HDLC)	DHCP, BOOTP, or Reverse Address Resolution Protocol (RARP)
Serial WAN interface with HDLC	Serial Line Address Resolution Protocol (SLARP)
Serial WAN interface with Frame Relay	BOOTP

If the server with the autoinstallation configuration file is not on the same LAN segment as the new device, or if a specific device is required by the network, you must configure an intermediate device directly attached to the new device through which the new device can send Trivial File Transfer Protocol (TFTP), BOOTP, and Domain Name System (DNS) requests. In this case, you specify the IP address of the intermediate device as the location to receive TFTP requests for autoinstallation.

Typical Autoinstallation Process on a New Device

When a device is powered on for the first time, it performs the following autoinstallation tasks:

1. The new device sends out DHCP, BOOTP, RARP, or SLARP requests on each connected interface simultaneously to obtain an IP address.

   If a DHCP server responds, it provides the device with some or all of the following information:

   - An IP address and subnet mask for the autoinstallation interface.
   - The location of the TFTP (typically), Hypertext Transfer Protocol (HTTP), or FTP server on which the configuration file is stored.
   - The name of the configuration file to be requested from the TFTP server.

- The IP address or hostname of the TFTP server.

  If the DHCP server provides only the hostname, a DNS server must be available on the network to resolve the name to an IP address.

- The IP address of an intermediate device if the configuration server is on a different LAN segment from the new device.

2. After the new device acquires an IP address, the autoinstallation process on the device attempts to download a configuration file in the following ways:

   a. If the DHCP server specifies the host-specific configuration file (boot file) ***hostname*.conf**, the device uses that filename in the TFTP server request. (In the filename, ***hostname*** is the hostname of the new device.) The autoinstallation process on the new device makes three unicast TFTP requests for ***hostname*.conf**. If these attempts fail, the device broadcasts three requests to any available TFTP server for the file.

   b. If the new device cannot locate ***hostname*.conf**, the autoinstallation process unicasts or broadcasts TFTP requests for a default device configuration file called **network.conf**, which contains hostname-to-IP address mapping information, to attempt to find its hostname.

   c. If **network.conf** contains no hostname entry for the new device, the autoinstallation process sends out a DNS request and attempts to resolve the new device's IP address to a hostname.

   d. If the new device can determine its hostname, it sends a TFTP request for the ***hostname*.conf** file.

   e. If the new device is unable to map its IP address to a hostname, it sends TFTP requests for the default configuration file **router.conf**.

3. After the new device locates a configuration file on a TFTP server, autoinstallation downloads the file, installs the file on the device, and commits the configuration.

NOTE:

- If you configure the DHCP server to provide only the TFTP server hostname, add an IP address-to-hostname mapping entry for the TFTP server to the DNS database file on the DNS server in the network.
- If the new device is not on the same network segment as the DHCP server (or other device providing IP address resolution), configure an existing device as an intermediate to receive TFTP and DNS requests and forward them to the TFTP server and the DNS server. You must configure the LAN or serial interface on the intermediate device with the IP addresses of the hosts providing TFTP and DNS service. Connect this interface to the new device.

Related Documentation

- Configuring Autoinstallation on J Series and SRX Series Devices on page 88

- Automatic Installation of Configuration Files (ACX Series Routers, J Series, and SRX Series Devices) on page 86
- *Installation and Upgrade Guide*

Automatic Installation of Configuration Files (ACX Series Routers, J Series, and SRX Series Devices)

Autoinstallation provides automatic configuration for a new device that you connect to the network and turn on, or for a device configured for autoinstallation.

Table 12 on page 86 lists the autoinstallation support on ACX Series Universal Access routers, SRX Series Secure Services Gateways devices, and J Series Services Routers.

Table 12: Autoinstallation Support

Platform	Autoinstallation
Branch SRX Series Devices	Yes
J Series Routers	Yes
ACX Series Routers	Yes

ACX Series Autoinstallation Overview

On ACX Series routers, autoinstallation enables you to deploy multiple routers from a central location in the network. Autoinstallation provides automatic configuration for a new router that you connect to the network and turn on, or for a router configured for autoinstallation. The autoinstallation process begins anytime a router is powered on and cannot locate a valid configuration file in the CompactFlash (CF) card. Typically, a configuration file is unavailable when a router is powered on for the first time, or if the configuration file is deleted from the CF card.

For more information about autoinstallation on the ACX Series, see *ACX Series Autoinstallation Overview*

J Series Automatic Installation Overview

On J Series routers, you can specify a remote server where configuration files are located. If a configuration file cannot be found on the router's CompactFlash card, the router automatically retrieves the configuration file from this remote server. For security purposes, you can encrypt these remote files using the DES cipher, and once they have been retrieved, the router decrypts them for use on the server.

To encrypt the files, we recommend the openSSL tool. You can get the open SSL tool at: http://www.openssl.org/. To encrypt the file, use the following syntax:

% openssl enc -des -k *passphrase* -in *original-file* -out *encrypted-file*

- ***passphrase***—Passphrase used to encrypt the configuration file. The passphrase should be the name of the file without the path information or file extension.
- ***original-file***—Unencrypted configuration file.
- ***encrypted-file***—Name of the encrypted configuration file.

For example, if you are encrypting the active configuration file **juniper.conf.gz**, the passphrase is **juniper.conf**. The openSSL syntax used to encrypt the file is:

```
% openssl enc -des -k juniper.conf -in juniper.conf.gz -out juniper.conf.gz.enc
```

SRX Services Gateway Automatic Installation Overview

The autoinstallation process begins any time a services gateway is powered on and cannot locate a valid configuration file in the internal flash. Typically, a configuration file is unavailable when a services gateway is powered on for the first time or if the configuration file is deleted from the internal flash. The autoinstallation feature enables you to deploy multiple services gateways from a central location in the network.

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over the network. You can use either the J-Web configuration editor or the CLI configuration editor to configure a device for autoinstallation.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the services gateway.

Autoinstallation takes place automatically when you connect an Ethernet port on a new services gateway to the network and power on the device. To simplify the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

Related Documentation

- Autoinstallation Overview (ACX Series Routers, J Series, and SRX Series Devices) on page 83
- *Installation and Upgrade Guide*

Configuring Autoinstallation on J Series and SRX Series Devices

This example shows how to configure a device for autoinstallation.

Requirements

Before you begin:

- Configure a DHCP server on your network to meet your network requirements. You can configure a device to operate as a DHCP server. See Example: Configuring the Device as a DHCP Server.
- Create one of the following configuration files, and store it on a TFTP server in the network (see "Configuration Files" on page 13):
  - A host-specific file with the name ***hostname*.conf** for each device undergoing autoinstallation. Replace ***hostname*** with the name of a device. The ***hostname*.conf**

file typically contains all the configuration information necessary for the device with this hostname.

  - A default configuration file named **router.conf** with the minimum configuration necessary to enable you to telnet into the new device for further configuration.

- Physically attach the device to the network using one or more of the following interface types:
  - Fast Ethernet
  - Gigabit Ethernet
  - Serial with HDLC encapsulation

Overview

No configuration is required on a device on which you are performing autoinstallation, because it is an automated process. However, to simplify the process, you can specify one or more interfaces, protocols, and configuration servers to be used for autoinstallation.

The device uses these protocols to send a request for an IP address for the interface.

- BOOTP—Sends requests over all interfaces.
- RARP—Sends requests over Ethernet interfaces.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit system
set autoinstallation configuration-servers ftp://user:password@sftpconfig.sp.com
set autoinstallation interfaces ge-0/0/0 bootp rarp
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a device for autoinstallation:

1. Enable autoinstallation and specify the URL address of one or more servers from which to obtain configuration files.

   ```
   [edit system]
   user@host# set autoinstallation configuration-servers
     ftp://user:password@sftpconfig.sp.com
   ```

2. Configure one or more Ethernet or serial interfaces to perform autoinstallation, and configure one or two procurement protocols for each interface.

   ```
   [edit system]
   user@host# set autoinstallation interfaces ge-0/0/0 bootp rarp
   ```

Results From configuration mode, confirm your configuration by entering the **show system autoinstallation status** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system autoinstallation status
```

```
Autoinstallation status:
Master state: Active
Last committed file: None
Configuration server of last committed file: 10.25.100.1
Interface:
  Name: ge-0/0/0
  State: Configuration Acquisition
  Acquired:
    Address: 192.168.124.75
    Hostname: host-ge-000
    Hostname source: DNS
    Configuration filename: router-ge-000.conf
    Configuration filename server: 10.25.100.3
  Address acquisition:
    Protocol: BOOTP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
```

If you are done configuring the device, enter **commit** from configuration mode.

NOTE: When there is a user-specified configuration for a particular interface, the factory default for that interface should be deleted. Having two configurations for the same device might lead to errors. For example, if PPP encapsulation is set on a T1 interface through user configuration while the factory default configuration configures CISCO HLDC on the same interface, then the interface might not come up and the following error will be logged in the message file: **"DCD_CONFIG_WRITE_FAILED failed."**

Verification

Confirm that the configuration is working properly.

- Verifying Autoinstallation on page 90

Verifying Autoinstallation

Purpose Verify that the device has been configured for autoinstallation.

Action From operational mode, enter the **show system autoinstallation status** command. The output shows the settings configured for autoinstallation. Verify that the values displayed are correct for the device when it is deployed on the network.

Related Documentation

- Autoinstallation Overview (ACX Series Routers, J Series, and SRX Series Devices) on page 83

- Automatic Installation of Configuration Files (ACX Series Routers, J Series, and SRX Series Devices) on page 86
- CLI Explorer
- *Installation and Upgrade Guide*

Autoinstallation of Satellite Devices in a Junos Node Unifier Group

In a Junos Node Unifier (JNU) group that contains an MX Series router as a controller that manages satellite devices, such as EX Series Ethernet Switches, QFX Series devices, and ACX Series Universal Access Routers, the autoinstallation functionality is supported for the satellite devices. JNU has an autoinstallation mechanism that enables a satellite device to configure itself out-of-the-box with no manual intervention, using the configuration available either on the network or locally through a removable media, or using a combination of both. This autoinstallation method is also called the *zero-touch* facility.

The zero-touch configuration delivers the following benefits:

- The router can be sent from the warehouse to the deployment site without any preconfiguration steps.
- The procedure required to deploy the device at the cell site is simplified, resulting in reduced operational and administrative costs.
- You can roll out large numbers of these devices in a very short time.

The factory default setting is autoinstallation-enabled. After you make the first configuration to the router, you can do either of the following:

- A JNU factory default file, **jnu-factory.conf**, is present in the **/etc/config/** directory and contains the configuration to perform autoinstallation on satellite devices. The zero-touch configuration can be disabled by including the **delete-after-commit** statement at the **[edit system autoinstallation]** hierarchy level and committing the configuration. This way, the saved configuration is used the next time the system reboots.
- Alternatively, if the router must get the configuration from the server each time a system reboot occurs, the zero-touch configuration must not be changed (that is, you must not include the **delete-after-commit** statement at the **[edit system autoinstallation]** hierarchy level and commit the settings).

Related Documentation

- *Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group*
- *Configuring Autoinstallation on JNU Satellite Devices*
- *Verifying Autoinstallation on JNU Satellite Devices*
- *autoinstallation*
- *delete-after-commit (JNU Satellites)*

- *configuration-servers*

CHAPTER 7

Configuring Dual-Root Partitions for High Availability

Understanding Resilient Dual-Root Partitions on Switches

Resilient dual-root partitioning, introduced on Juniper Networks EX Series Ethernet Switches in Juniper Networks Junos operating system (Junos OS) Release 10.4R3, provides additional resiliency to switches in the following ways:

- Allows the switch to boot transparently from the second (alternate) root partition if the system fails to boot from the primary root partition.
- Provides separation of the root Junos OS file system from the **/var** file system. If corruption occurs in the **/var** file system (a higher probability than in the root file system because of the greater frequency of reads and writes in **/var**), the root file system is insulated from the corruption.

NOTE: **For instructions on upgrading to a release that supports resilient dual-root partitions from a release that does not, see the release notes. The procedure for upgrading to a resilient dual-root partition release is different from the normal upgrade procedure.**

This topic covers:

Resilient Dual-Root Partition Scheme (Junos OS Release 10.4R3 and Later)

EX Series switches that ship with Junos OS Release 10.4R3 or later are configured with a root partition scheme that is optimized for resiliency, as shown in Table 13 on page 94.

Table 13: Resilient Dual-Root Partition Scheme

Slice 1	Slice 2	Slice 3		Slice 4
s1a	s2a	s3e	s3d	s4d
/ (root Junos OS)	**/** (root Junos OS)	**/var**	**/var/tmp**	**/config**

In the resilient dual-root partition scheme, the **/var** file system is contained in a separate slice (Slice 3) from the root file systems; the **/config** directory is contained in its own slice (Slice 4); and switches ship from the factory with identical Junos OS images in Slice 1 and Slice 2. The **/var** file system, which has a greater frequency of reads and writes than the root file systems and is therefore more likely to have corruption issues, is isolated from the root directories and the **/config** directory. If the switch fails to boot from the active partition, the switch automatically boots from the alternate root partition and triggers an alarm.

Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature

Resilient dual-root partitioning also provides the *automatic snapshot* feature, which allows the switch to automatically fix a corrupt Junos OS file in the primary root partition. If the automatic snapshot feature is enabled, the switch automatically takes a snapshot of the Junos OS root file system in the alternate root partition and copies it onto the primary root partition, thereby repairing the corrupt file in the primary root partition. The automatic snapshot procedure takes place whenever the system reboots from the alternate root partition, regardless of whether the reboot is due to a command or due to corruption of the primary root partition.

NOTE:

- EX9200 switches do not support the automatic snapshot feature.
- The automatic snapshot feature is enabled by default on the following EX Series switches:
  - EX4550 switches
  - EX Series switches that ship with Junos OS Release 12.3R1 or later
- The automatic snapshot feature is disabled by default on EX Series switches (except the EX4550 switches) running Junos OS Release 12.2 or earlier.
- If the automatic snapshot feature was disabled by default before the switch was upgraded to Junos OS Release 12.3R1 or later, the feature remains disabled (for backward compatibility) by default after the upgrade.
- If the automatic snapshot feature is enabled in a Virtual Chassis configuration, the automatic snapshot procedure takes place whenever any member of the Virtual Chassis reboots from its alternate root partition.
- You can enable the automatic snapshot feature by configuring the auto-snapshot statement at the **[edit system]** hierarchy level.

The automatic snapshot feature provides an additional layer of fault protection if you maintain the same version of Junos OS in both partitions of resilient dual-root partitions. When **auto-snapshot** is enabled, repair happens automatically. Therefore, the switch does not issue an alarm to indicate that the system has rebooted from the alternate partition. However, it does log the event. You cannot execute a manual snapshot when an automatic snapshot procedure is in process. The login banner indicates that an automatic snapshot operation is in progress and that banner is removed only after the snapshot operation is complete. The next reboot happens from the primary partition.

NOTE: EX Series switches that ship with Junos OS Release 10.4R3 or later are configured with identical Junos OS images in the primary root partition (Slice 1) and the alternate root partition (Slice 2).

However, if you do *not* maintain the same version of Junos OS in both partitions, you might want to disable the automatic snapshot feature. If you have an earlier version of Junos OS in the alternate partition and the system reboots from the alternate root partition, the automatic snapshot feature causes the later Junos OS version to be replaced with the earlier version.

When automatic snapshot is disabled and the system reboots from the alternate root partition, it triggers an alarm indicating that the system has rebooted from its alternate partition.

Earlier Partition Scheme (Junos OS Release 10.4R2 and Earlier)

The partition scheme used in Junos OS 10.4R2 and earlier is shown in Table 14 on page 96.

Table 14: Earlier Partition Scheme

Slice 1		Slice 2		Slice 3	
s1a	s1f	s2a	s2f	s3d	s3e
/ (root Junos OS)	**/var**	(empty until initial software upgrade)	(empty until initial software upgrade)	**/var/tmp**	**/config**

This is the partitioning scheme for a switch shipped with Release 10.4R2 or earlier (or after you reformat the disk during a downgrade from Release 10.4R3 or later to Release 10.4R2 or earlier). In this partitioning scheme, the switch comes from the factory with only one Junos OS image installed in the root Junos OS partition of Slice 1. The first time that you perform a software upgrade, the new Junos OS image is installed in Slice 2. If the switch fails to boot, you must manually trigger it to boot from the alternate partition (rebooting from the alternate partition does not occur automatically).

Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases

Upgrading from Release 10.4R2 or earlier to Release 10.4R3 or later differs from other upgrades in two important ways:

- You must install a new loader software package in addition to installing the new Junos OS image.
- Rebooting after the upgrade reformats the disk from three partitions to four partitions. See Table 13 on page 94.

You can perform all operations for this special software upgrade from the CLI.

CAUTION: **Back up any important log files because the /var/log files are not saved or restored during an upgrade from Release 10.4R2 or earlier to a release that supports resilient dual-root partitions (Release 10.4R3 or later).**

We recommend that you also save your /config files and any important log files to an external medium because if there is a power interruption during the upgrade process, they might be lost.

Related Documentation

- Resilient Dual-Root Partitions Frequently Asked Questions on page 102
- *EX Series Virtual Chassis Overview*
- *EX8200 Virtual Chassis Overview*

Dual-Root Partitioning Scheme on SRX Series Devices

Junos OS Release 10.0 and later support dual-root partitioning on SRX Series devices. Dual-root partitioning allows the SRX Series device to remain functional even if there is file system corruption and to facilitate easy recovery of the file system.

SRX Series devices running Junos OS Release 9.6 or earlier support a single-root partitioning scheme where there is only one root partition. Because both the primary and backup Junos OS images are located on the same root partition, the system fails to boot if there is corruption in the root file system. The dual-root partitioning scheme guards against this scenario by keeping the primary and backup Junos OS images in two independently bootable root partitions. If the primary root partition becomes corrupted, the system can still boot from the backup Junos OS image located in the other root partition and remain fully functional.

SRX Series devices that ship with Junos OS Release 10.0 or later are formatted with dual-root partitions from the factory. SRX Series devices that are running Junos OS Release 9.6 or earlier can be formatted with dual-root partitions when they are upgraded to Junos OS Release 10.0 or later.

NOTE: **Although you can install Junos OS Release 10.0 or later on SRX Series devices with the single-root partitioning scheme, we strongly recommend the use of the dual-root partitioning scheme.**

This section contains the following topics:

Boot Media and Boot Partition on the SRX Series Devices

When the SRX Series device powers on, it tries to boot the Junos OS from the default storage media. If the device fails to boot from the default storage media, it tries to boot from the alternate storage media.

Table 15 on page 98 provides information on the storage media available on SRX Series devices.

Table 15: Storage Media on SRX Series Devices

SRX Series Devices	Storage Media
SRX100, SRX210, and SRX240	• Internal NAND flash (default; always present) • USB storage device (alternate)
SRX650	• Internal CF (default; always present) • External flash card (alternate) • USB storage device (alternate)

With the dual-root partitioning scheme, the SRX Series device first tries to boot the Junos OS from the primary root partition and then from the backup root partition on the default storage media. If both primary and backup root partitions of a media fail to boot, then the SRX Series device tries to boot from the next available type of storage media. The SRX Series device remains fully functional even if it boots the Junos OS from the backup root partition of the storage media.

Important Features of the Dual-Root Partitioning Scheme

The dual-root partitioning scheme has the following important features:

- The primary and backup copies of Junos OS images reside in separate partitions. The partition containing the backup copy is mounted only when required. With the single-root partitioning scheme, there is one root partition that contains both the primary and the backup Junos OS images.
- The **request system software add** command for a Junos OS package erases the contents of the other root partition. The contents of the other root partition will not be valid unless software installation is completed successfully.
- Add-on packages, such as **jais** or **jfirmware**, can be reinstalled as required after a new Junos OS image is installed.
- The **request system software rollback** command does not delete the current Junos OS image. It is possible to switch back to the image by issuing the **rollback** command again.
- The **request system software delete-backup** and **request system software validate** commands do not take any action.

Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning

The auto-snapshot feature repairs the corrupted primary root when the device reboots from the alternate root. This is accomplished by taking a snapshot of the alternate root onto the primary root automatically rather than manually from the CLI.

```
login: user

Password:

***********************************************************************

**                                                                   **
```

```
**  WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE      **
**                                                                   **
**  It is possible that the primary copy of JUNOS failed to boot up   **
**  properly, and so this device has booted from the backup copy.    **
**                                                                   **
**  The primary copy will be recovered by auto-snapshot feature now. **
**                                                                   **
***********************************************************************
```

When this feature is enabled, and the device reboots from the alternate root (because of a corrupted primary root or power cycle during restart), the following actions take place:

1. A prominent message is displayed indicating a failure to boot from the primary root.
2. A system **boot from backup root** alarm is set. This is useful for devices that do not have console access.
3. A snapshot of the alternate root onto the primary root is made.
4. Once the snapshot is complete, the system **boot from backup root** alarm is cleared.

During the next reboot, the system determines the good image on the primary root and boots normally.

By default the auto-snapshot feature is disabled.

If you do want to maintain different Junos OS versions on the partition, this feature can be enabled by default.

If you want to keep two different versions of a Junos OS image, this feature can be disabled by default.

NOTE: **We recommend performing the snapshot once all the processes start. This is done to avoid any increase in the reboot time.**

Enable this feature with the **set system auto-snapshot** command. Once the primary root partition is recovered using this method, the device will successfully boot from the primary root partition on the next reboot.

Execute the **delete system auto-snapshot** command to delete all backed up data and disable auto-snapshot, if required.

Use the **show system auto-snapshot** command to check the auto-snapshot status.

When auto-snapshot is in progress, you cannot run a manual snapshot command concurrently and the following error message appears:

```
Snapshot already in progress. Please try after sometime.
```

NOTE: If you log into the device when the snapshot is in progress, the following banner appears: **The device has booted from the alternate partition, auto-snapshot is in progress.**

Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers Devices

If the SRX Series Services Gateway is unable to boot from the primary Junos OS image, and boots up from the backup Junos OS image in the backup root partition, a message appears on the console at the time of login indicating that the device has booted from the backup Junos OS image.

```
login: user

Password:

***********************************************************************

**                                                                   **

**  WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE      **

**                                                                   **

**  It is possible that the active copy of JUNOS failed to boot up   **

**  properly, and so this device has booted from the backup copy.    **

**                                                                   **

**  Please re-install JUNOS to recover the active copy in case       **

**  it has been corrupted.                                           **

**                                                                   **

***********************************************************************
```

Because the system is left with only one functional root partition, you should immediately restore the primary Junos OS image using one of the following methods:

- Install a new image using the CLI or J-Web user interface. The newly installed image will become the primary image, and the device will boot from it on the next reboot.
- Use a snapshot of the backup root partition by entering the **request system snapshot slice alternate** command. Once the primary root partition is recovered using this method, the device will successfully boot from the primary root partition on the next reboot.

After the procedure, the primary root partition will contain the same version of Junos OS as the backup root partition.

NOTE: You can use the CLI command **request system snapshot slice alternaterequest system snapshot slice alternate** to back up the currently running root file system (primary or secondary) to the other root partition on the system.

You can use this command to:

- Save an image of the primary root partition in the backup root partition when system boots from the primary root partition.
- Save an image of the backup root partition in the primary root partition when system boots from the backup root partition.

WARNING: The process of restoring the alternate root by using the CLI command **request system snapshot slice alternate** takes several minutes to complete. If you terminate the operation before completion, the alternate root might not have all required contents to function properly.

Understanding Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning

NOTE: If you are upgrading to Junos OS Release 10.0 without transitioning to dual-root partitioning, use the conventional CLI and J-Web user interface installation methods.

To format the media with dual-root partitioning while upgrading to Junos OS Release 10.0 or later, use one of the following installation methods:

- Installation from the boot loader using a TFTP server. We recommend this if console access to the system is available and a TFTP server is available in the network. See "Installing Junos OS on SRX Series Devices (Using Boot Loader and USB)" on page 66
- Installation from the boot loader using a USB storage device. We recommend this method if console access to the system is available and the system can be physically accessed to plug in a USB storage device. See "Installing Junos OS on SRX Series Devices (Using Boot Loader and USB)" on page 66
- Installation from the CLI using the **partition** option. We recommend this method only if console access is not available. This installation can be performed remotely.

NOTE: After upgrading to Junos OS Release 10.0 or later, the U-boot and boot loader must be upgraded for the dual-root partitioning scheme to work properly.

Related Documentation

- Understanding Junos OS Upgrades for J Series and SRX Series Devices on page 188
- Reinstalling the Single-Root Partition on SRX Series Devices on page 272
- Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 71
- *Installation and Upgrade Guide*

Resilient Dual-Root Partitions Frequently Asked Questions

NOTE: This task uses Junos OS for EX Series switches that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Resilient Dual-Root Partitions Frequently Asked Questions*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

This FAQ addresses questions regarding resilient dual-root partitions on EX Series switches and upgrading to Junos OS releases that support resilient dual-root partitions. The resilient dual-root partition feature was introduced on EX Series switches at Junos OS Release 10.4R3. It provides additional resiliency for EX Series switches.

This FAQ covers the following questions:

How Does Upgrading to Junos OS Release 10.4R3 and Later Differ from Normal Upgrades?

Upgrading from Junos OS Release 10.4R2 or earlier to Release 10.4R3 or later differs from other upgrades in these ways:

- You must upgrade the loader software in addition to installing the new Junos OS image.
- Rebooting after the upgrade reformats the disk from three partitions to four partitions.
- The upgrade process and the reboot take longer time because of the additional time required for upgrading the loader software and for the first reboot after the Junos OS installation (longer than normal because it reformats the disk from three partitions to four). Also, EX8200 switches require an additional reboot per Routing Engine as part of the loader software upgrade.

What Happens If I Do Not Upgrade Both the Loader Software and Junos OS at the Same Time?

You must install a new loader software package if you are upgrading to a release that supports resilient dual-root partitions (Release 10.4R3 and later) from an earlier release (Release 10.4R2 and earlier).

If you upgrade to Release 10.4R3 or later from Release 10.4R2 or earlier and do not upgrade the loader software, the switch will come up and function normally. However, if the switch encounters a problem and cannot boot from the active root partition, it cannot transparently boot from the alternate root partition and you will need to perform a manual reboot.

NOTE: **Starting with Junos OS Release 11.4R4, when an EX Series switch boots from the flash memory, and a valid jloader firmware image does not exist or is corrupted in the upgrade bank, the following alarm is displayed: "Upgrade bank is empty or corrupted for FPC 0, please do standard upgrade sequence." To resolve this issue, contact JTAC for assistance in determining the version of jloader firmware that you need to install.**

Table 16: Combinations of Junos OS Versions and Loader Software Versions

Junos OS Release	Loader Software	Notes
Release 10.4R3 and later	New loader software For all EX Series switches except EX8200 switches: **U-Boot 1.1.6 (Mar 11 2011 - 04:39:06) 1.0.0** (Contains version 1.0.0 after the timestamp.) For EX8200 switches: **U-Boot 1.1.6 (Jan 11 2008 - 05:24:35) 3.5.0** (Contains version 3.5.0.)	Recommended

Table 16: Combinations of Junos OS Versions and Loader Software Versions *(continued)*

Junos OS Release	Loader Software	Notes
Release 10.4R2 and earlier	Old loader software	If you downgrade to Release 10.4R2 or earlier after having upgraded to the new loader software version, you do not need to downgrade the loader software. The switch will function normally.
Release 10.4R3 and later	Old loader software For all EX Series switches except EX8200 switches: **U-Boot 1.1.6 (Jan 11 2008 - 05:24:35)** (Does not contain a version number after the timestamp) For EX8200 switches: **U-Boot 1.1.6 (Jan 11 2008 - 05:24:35) 2.3.0** (Contains a version earlier than 3.5.0.)	The switch will come up and function normally. However, in the event that the switch cannot boot from the active root partition, it will not transparently boot up from the alternate root partition.
Release 10.4R2 and earlier	New loader software NOTE: For EX Series switches except EX8200 switches, in Release 10.4R2 and earlier the version number after the timestamp (shown in the previous row) is not displayed, and you cannot verify whether the old or the new loader software version is installed.	The switch will come up and function normally.

Can I Downgrade Junos OS Without Downgrading the Loader Software?

Yes, when you downgrade from most releases, the new loader software runs seamlessly with the earlier Junos OS version.

NOTE: If you downgrade specifically from Release 10.4R3 or Release 11.1R1 to 10.4R2 or earlier (that is, to a release that does not support resilient dual-root partitions), you must disable the boot-sequencing function. If you do not take this action, the switch will boot on each subsequent reboot from the alternate root partition rather than from the active partition.

Disable the boot-sequencing function in one of two ways:

- From the shell as the root user:

  % **nvram setenv boot.btsq.disable 1**

- From a console connection, reboot and stop at the u-boot prompt (Ctrl+c):

  => **setenv boot.btsq.disable 1**
  => **savenv**

If you are downgrading from Release 10.4R4 or from Release 11.1R2 or later to Release 10.4R2 or earlier, you do not need to disable the boot-sequencing function—the software does it automatically.

Can I Upgrade to a Resilient Dual-Root Partition Release by Using the CLI?

Yes, you can perform the entire upgrade to resilient dual-root partitions from the CLI. You download both the new loader software and Junos OS packages and install them from the CLI. During the final reboot, the disk is automatically reformatted from three to four partitions.

Will I Lose My Configuration During an Upgrade?

Configuration files are preserved and restored during the reformatting of the disk. We recommend that you save your configuration before upgrading because if there is a power interruption during the installation process, the files might be lost.

How Long Will the Upgrade Process Take?

The process of upgrading to a resilient dual-root partition release takes longer than other upgrades because of the additional step of upgrading the loader software and the longer reboot time required while the disk is reformatted to four partitions during the reboot of the switch that completes the Junos OS upgrade. The reformat results in an additional reboot time of 5 to 10 minutes for EX2200, EX3200, EX4200, and EX4500 switches. For EX8200 switches, the reboot time increases by 10 to 25 minutes per Routing Engine, and additional reboots are required.

What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot is Enabled?

If the automatic snapshot feature is enabled during a reboot, the system automatically takes a snapshot of Junos OS from the alternate root partition (Slice 2) and copies it onto the primary root partition (Slice 1). The system checks each file system partition for corruption. Table 17 on page 105 shows the action the system takes if corruption is detected and the corrective action that you can take.

Table 17: Actions If Corrupt Files Are Found and Automatic Snapshot is Enabled

Slice 1	Slice 2	Slice 3		Slice 4
s1a	s2a	s3e	s3d	s4d
/ (root Junos OS)	**/** (root Junos OS)	**/var**	**/var/tmp**	**/config**
If a root directory (**/**) is corrupted, the corrupted file system is not mounted. The switch automatically takes a snapshot of the Junos OS root file system and copies it onto the primary root partition. It boots from the alternate slice, but the next reboot happens from the primary slice.		During early boot, the integrity of **/var**, **/var/tmp**, and **/config** files is verified. If they are corrupted, the corrupted slice is reformatted and the file directory in that slice is lost.		

Table 17: Actions If Corrupt Files Are Found and Automatic Snapshot is Enabled *(continued)*

Slice 1	Slice 2	Slice 3		Slice 4
s1a	s2a	s3e	s3d	s4d
Corrective action: No corrective action is required.		Corrective action: Restore the **/var** or **/config** files from the external backup.		

What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot is Not Enabled?

During a reboot, the system checks each file system partition for corruption. Table 18 on page 106 shows the action the system takes if corruption is detected and the corrective action that you can take.

Table 18: Actions If Corrupt Files Are Found

Slice 1	Slice 2	Slice 3		Slice 4
s1a	s2a	s3e	s3d	s4d
/ (root Junos OS)	**/** (root Junos OS)	**/var**	**/var/tmp**	**/config**
If a root directory (**/**) is corrupted, the corrupted file system is not mounted and the switch boots from the alternate slice.		During early boot, the integrity of **/var**, **/var/tmp**, and **/config** files is verified. If they are corrupted, the corrupted slice is reformatted and the file directory in that slice is lost.		
Corrective action: Issue a request system snapshot command from the good root directory to the corrupted slice.		Corrective action: Restore the **/var** or **/config** files from the external backup.		

How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System?

If the switch detects corruption in the primary root file system, it boots from the alternate root partition. When this occurs, the type of notification depends on whether you have enabled the automatic snapshot feature or not:

- If the automatic snapshot feature is not enabled:
  - If you are logged in through the console port or the management port:

```
WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE

It is possible that the primary copy of JUNOS failed to boot up
properly, and so this device has booted from the backup copy.

Please re-install JUNOS to recover the primary copy in case
it has been corrupted.
```

- The following message is displayed when you issue **show chassis alarms**:

```
user@switch> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2011-02-17 05:48:49 PST  Minor  Host 0 Boot from backup root
```

- If the automatic snapshot feature is enabled:
  - A banner message appears, indicating that an automatic snapshot operation is in progress. The banner message disappears when the snapshot operation is complete.
  - No alarm is issued to indicate that the switch has been rebooted from the alternate partition. However, the switch does log the event.

Can I Use Automatic Software Update and Download to Upgrade to a Resilient Dual-Root Partition Release?

Automatic software update and automatic software download are both supported with upgrading to releases that support resilient dual-root partitions. However, after an automatic installation, you must take the extra step of upgrading the loader software.

Automatic software update is for new members added to a Virtual Chassis that do not have the same software as the master. Once this feature is configured on the Virtual Chassis, any new member added with a different software version will be upgraded automatically.

Automatic software download uses the DHCP message exchange process to download and install software packages.

Why Is the Message "At least one package installed on this device has limited support" Displayed When Users Log In to a Switch?

The following message might be displayed when a user logs in:

```
Logging to master
         ..Password:
         --- JUNOS 10.4R3.4 built 2011-03-19 22:06:32 UTC
        At least one package installed on this device has limited support.
        Run 'file show /etc/notices/unsupported.txt' for details.
```

This message can be safely ignored or you can permanently remove it. It appears because the jloader package file has been detected, and it only appears when Junos OS is installed before the loader software is upgraded (required only for EX8200 switches).

You can permanently remove this message by removing the jloader package and rebooting the system:

```
user@switch> request system software delete jloader-ex-zzzz
user@switch> request system reboot
```

Where *jloader-ex-zzzz* represents the name of the jloader software package for your platform—jloader-ex2200 for an EX2200 switch, jloader-ex3242 for an EX3200 or EX4200 switch, or jloader-ex8200 for an EX8200 switch.

Where Can I Find Instructions for Upgrading?

The procedure for upgrading to a release that supports resilient dual-root partitions (from a release that does not) is different from the normal upgrade procedure. For instructions on upgrading to a resilient dual-root partition release, see the Release Notes.

Related Documentation

- Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 180
- Troubleshooting Software Installation on page 321
- Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 324
- Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 180

CHAPTER 8

Upgrading Software

Upgrading Software Packages

NOTE: When you install individual software packages, the following notes apply:

- When upgrading from Junos OS Release 8.2 or earlier to Junos OS Release 8.5, use the **system software add** *<image>* **no-validate** command option.
- Only use the **jinstall** Junos OS image when upgrading or downgrading to or from Junos OS Release 8.5. Do not use the **jbundle** image.
- Before upgrading to Junos OS Release 8.5, ensure that the routing platform's CompactFlash card is 256 MB or larger to avoid disk size restrictions. (M7i routers without a CompactFlash card are excluded.)

To upgrade an individual Junos OS package, follow these steps:

1. Download the software packages you need from the Juniper Networks Support Web site at **http://www.juniper.net/support/**. For information about downloading software packages, see "Downloading Software" on page 40.

   NOTE: We recommend that you upgrade all individual software packages using an out-of-band connection from the console or management Ethernet interface, because in-band connections can be lost during the upgrade process.

2. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

   user@host> **request system snapshot**

   The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router's hard disk or solid-state drive (SSD).

NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software, because the running copy and the backup copy of the software are identical.

3. If you are copying multiple software packages to the router, copy them to the **/var/tmp** directory on the hard disk or solid-state drive (SSD):

   user@host> **file copy ftp**://*username* :prompt@ftp.*hostname* .net/*filename*/var/tmp/*filename*

4. Add the new software package:

   - To add an individual software package:

     user@host> **request system software add**/var/tmp/ *installation-package* validate

     installation-package is the full URL to the file.

     If you are upgrading more than one package at the same time, add **jbase** first. If you are using this procedure to upgrade all packages at once, add them in the following order:

     user@host> **request system software add** /var/tmp/jbase-*release*-signed.tgz

     user@host> **request system software add** /var/tmp/jkernel-*release*-signed.tgz

     user@host> **request system software add** /var/tmp/jpfe-*release*-signed.tgz

     user@host> **request system software add** /var/tmp/jdocs-*release*- signed.tgz

     user@host> **request system software add** /var/tmp/jweb-*release*- signed.tgz

     user@host> **request system software add** /var/tmp/jroute-*release*-signed.tgz

     user@host> **request system software add** /var/tmp/jcrypto-*release*-signed.tgz

   - For M Series, MX Series, and T Series routers and Branch SRX Series firewall filters running Junos OS Release 12.2 and above, you can add more than one software package at the same time. To add multiple software packages:

     user@host> **request system software add set** /var/tmp/ *installation-package*/var/tmp/ *installation-package* validate

     installation-package can be any of the following:

     - A list of installation packages, each separated by a blank space. For example,

       user@host> **request system software add set** /var/tmp/ *jinstall-10.2R1.8–domestic-signed.tgz* /var/tmp/ *jtools*.tgz* validate

     - The full URL to the directory or tar file containing the list of installation packages.

     Use the **request system software add set** command to retain any SDK configuration by installing the SDK add-on packages along with the core Junos OS installation package.

     WARNING: Do not include the *re0* | *re1* option when you install a package using the **request system software add** command, if the Routing Engine on

which the package is located and the Routing Engine on which you want to install the package are the same. In such cases, the package gets deleted after a successful upgrade.

The system might display the following message:

```
pkg_delete: couldn't entirely delete package
```

This message indicates that someone manually deleted or changed an item that was in a package. You do not need to take any action; the package is still properly deleted.

For more information about the **request system software add** command, see the CLI Explorer.

5. Reboot the router to start the new software:

   user@host> **request system reboot**

6. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the **request system snapshot** command to back up the new software:

   user@host> **request system snapshot**

   NOTE: On an ACX router, you must issue the **request system snapshot slice alternate** command.

   The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router's hard disk or solid-state drive (SSD).

   NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software, because the running copy and backup copy of the software are identical.

Upgrading Software

To upgrade Junos OS, you need to install the appropriate upgrade package on the device. Upgrading involves these tasks:

NOTE: If you want to use the Open Network Install Environment (ONIE) to install software, see *Installing and Recovering Software Using the Open Network Install Environment (ONIE)*.

1. Downloading Software Files with a Browser on page 113
2. Accessing Software Downloaded to a Remote Location on page 114

Downloading Software Files with a Browser

To download the software package from the Juniper Networks Support website, go to http://www.juniper.net/support/ .

NOTE: To access the download site, you must have a service contract with Juniper Networks and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website https://www.juniper.net/registration/Register.jsp .

This procedure shows you how to upgrade software on a QFX Series device, but you can follow the same procedure for any device unless otherwise specified.

1. Using a Web browser, navigate to the http://www.juniper.net/support .
2. Click **Download Software**.
3. In the **Switching** box, click **Junos OS Platforms**.
4. In the **QFX Series** section, click the name of the platform for which you want to download software.
5. Click the **Software** tab and select the release number from the **Release** drop-down list.
6. In the **Install Package** section of the **Software** tab, select the **Install Package** for the release.

   A login screen appears.
7. Enter your name and password and press **Enter**.
8. Read the End User License Agreement, click the **I agree** radio button, and then click **Proceed**.
9. Save the **jinstall-qfx-<*version*>-domestic-signed.tgz** file on your computer.
10. Open or save the installation package either to the local system in the **var/tmp** directory or to a remote location. If you are saving the installation package to a remote system, make sure that you can access it using HTTP, TFTP, FTP, or scp.

Accessing Software Downloaded to a Remote Location

To access the installation package if you downloaded it to a remote location (for example, any system other than the switch), you can access the package using the CLI. You can specify a filename or URL in one of the following ways:

1. Copy a file from an FTP server, TFTP, or scp session.

   In this example, a file is copied from an FTP server using the **file copy** command.

2. Enter the file name on the prompt of a file on an FTP server. You can also specify ***hostname*** as ***username*@*hostname*** or ***username*:*password*@*hostname***. The default path is the user's home directory. To specify an absolute path, the path must start with **%2F**; for example, **ftp***://hostname/%2Fpath/filename*. To have the system prompt you for the password, specify **prompt** in place of the password. If a password is required and you do not specify the password or **prompt**, an error message is displayed:

   ```
   user@host> file copy ftp://username@ftp.hostname.net/package-name-m.mZx-distribution
   .tgz
   file copy ftp.hostname.net: Not logged in.
   ```

   ```
   user@host> file copy
   ftp://username:prompt@ftp.hostname.net/package-name-m.mZx-distribution
   Password for username@ftp.hostname.net:
   ```

Connecting to the Console Port

We recommend that you connect to the console port while installing the installation package so you can respond to any required user input and detect any errors that may occur.

Backing Up the Current Configuration Files

Before you install the new installation package, we strongly recommend that you back up your current configuration files because the upgrade process removes all of the stored files on the switch.

To back up your current configuration files, enter the **save** command:

```
user@switch# save filename
```

Executing this command saves a copy of your configuration files to a remote location such as an external USB device.

Installing a Standard Software Package

NOTE: On Junos Release 14.1X53-D35.3, autonegotation is disabled by default.

NOTE: Before you install the software, back up any critical files in /var/home. For more information regarding how to back up critical files, contact Customer Support at http://www.juniper.net/support.

NOTE: If you are upgrading from a standard software package to an ELS-based package, see the *Upgrading to an ELS-Based Software Package* section.

Install the software in one of three ways:

NOTE: On the switch, use the **force-host** option to force installing the latest version of the Host OS.

If the installation package resides locally on the switch, execute the **request system software add force-host** *<pathname><source>* **reboot** command.

For example:

```
user@switch> request system software add force-host /var/tmp/jinstall-qfx-11.1R1.5-domestic.tgz
reboot
```

If the Install Package resides remotely, execute the **request system software add force-host** *<pathname><source>* **reboot** command.

For example:

```
user@switch> request system software add force-host
ftp://ftpserver/directory/jinstall-qfx-11.1R1.5-domestic.tgz reboot
```

If the installation package resides locally on the switch, execute the **request system software add force-host** *<pathname><source>* **reboot** command.

For example:

```
user@switch> request system software add force-host
/var/tmp/jinstall-qfx-5.13.2X51-D10.6-domestic.tgz reboot
```

If the install Package resides remotely from the switch, execute the **request system software add force-host** *<pathname><source>* **reboot** command.

For example:

```
user@switch> request system software add force-host
ftp://ftpserver/directory/jinstall-qfx-5.13.2X51-D10.6-domestic.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Upgrading to an ELS-Based Software Package

To upgrade your switch from a version of Junos OS that does not support Enhanced Layer 2 Software (ELS) to a version of Junos OS that supports ELS, we recommend performing the following procedure.

NOTE: Because this procedure can cause service outages, we recommend that you avoid performing this procedure on switches carrying traffic in a production network.

1. Log in to your device using the console port.

NOTE: Only perform this procedure from the console port. You can lose connectivity to your device if you perform this procedure from a management port or any other interface.

2. Set your device to standalone mode by issuing the **request chassis device-mode standalone** command. Do not reboot your system at this time.

   NOTE: This step is only required for new devices shipped from the factory or QFabric system Node devices that you plan to redeploy in a QFX Series Virtual Chassis.

3. Choose whether you wish to reuse your previous configuration or not.

   - To reuse your previous configuration as part of the software upgrade, you must convert the configuration from the original style Junos OS CLI to the ELS CLI format using the following steps:

     NOTE: We recommend this procedure for customers currently using a QFX3500 or QFX3600 switch as a standalone device.

     a. Copy your entire existing configuration into a text file. Save the file to a remote location or USB drive.

     b. Retain the portion of your existing configuration related to management network connectivity (such as **[edit system]** and management interfaces). Delete all other configuration elements (such as the **[edit protocols]** and **[edit vlans]** hierarchy levels, non-management interfaces, and so on). Issue a **commit** operation to remove the deleted configuration.

     c. Perform the software upgrade with the **validate** option and reboot your device to complete the upgrade by issuing the **request system software add validate reboot** command. Maintain your console port connection during the reboot.

     d. Using a web browser, navigate to the ELS Translator Tool. Follow the instructions on the page to convert your saved configuration file to the new ELS CLI format.

     e. Return to your console port connection. When the switch has rebooted to complete the software upgrade, copy the configuration from the ELS Translator Tool and load it in to your switch.

     f. Issue a **commit** operation to activate the translated configuration.

   - To delete your current configuration and upgrade the software, follow these steps:

     NOTE: We recommend this procedure for customers with new QFX3500 or QFX3600 devices shipped from the factory or QFabric system Node devices that will be redeployed in a QFX Series Virtual Chassis.

a. Perform a software upgrade with the **no-validate** option by issuing the **request system software add no-validate** command.

b. Delete the configuration and set the device to factory defaults by issuing the **request system zeroize** command. The device automatically reboots and reverts to a factory default configuration.

c. Configure your device using the ELS CLI format.

Related Documentation

- *Installing and Recovering Software Using the Open Network Install Environment (ONIE)*
- Overview of CoS Upgrade Requirements (Junos OS Release 11.1 or 11.2 to a Later Release) on page 205
- *Software Installation Overview*
- *Recovering from a Failed Software Installation*
- *Upgrading Jloader Software on QFX Series Devices*
- **request system software add on page 373**
- *Installation and Upgrade Guide*

Upgrading to 64-bit Junos OS

Just like any other operating system, the 64-bit version of Junos OS can address more memory than the 32-bit version of the operating system. In order to support larger Routing Engine memory sizes, an upgrade from the 32-bit to the 64-bit Junos OS running on the Routing Engine hardware is necessary. The upgrade path is relatively straightforward and another form of Routing Engine hardware and software upgrade. However, there are three different and distinct Routing Engine configurations that must be taken into account when upgrading to the 64-bit Junos OS. This topic covers all three.

The In Service Software Upgrade (ISSU) procedure is not supported while upgrading from the 32-bit version of Junos OS to the 64-bit version of Junos OS. The upgrade process involves some downtime, so traffic will be affected.

NOTE: **The 64-bit version of Junos OS is not supported on every Routing Engine. To determine whether your router and Routing Engine support a 64-bit version of Junos OS, see *Supported Routing Engines by Router*.**

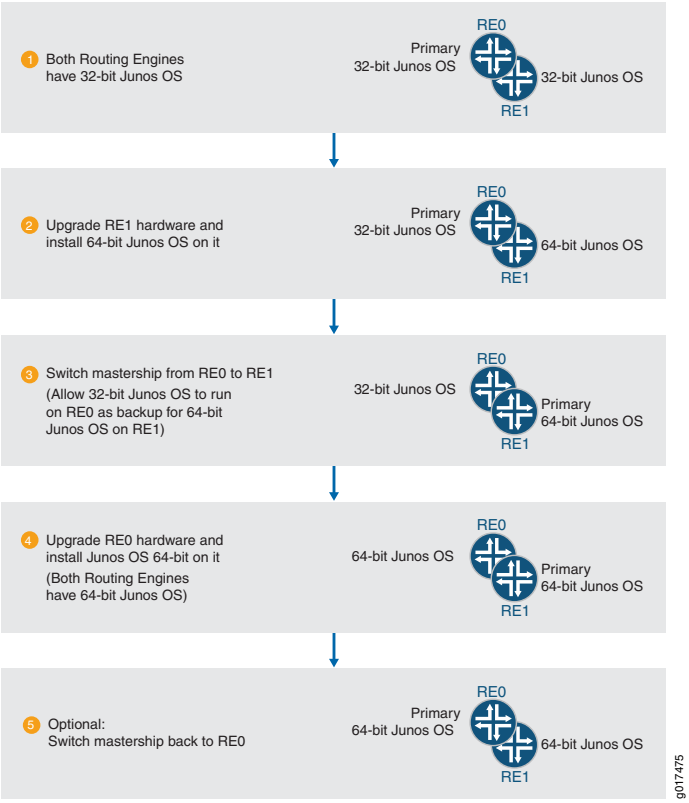
Before you begin, you must have:

- A properly configured and functional router
- One or two Routing Engines installed that support the 64-bit Junos OS
- Decided to allow single Routing Engines systems to use either slot 0 or slot 1 as master or not (this decision will determine which upgrade path to follow for single Routing Engine systems)

When you upgrade a Routing Engine to the 64-bit Junos OS, you can support larger Routing Engine memory sizes. However, the exact procedure depends on whether there are one or two Routing Engines installed. For systems with a single Routing Engine, the procedure varies based on whether the master Routing Engine must always be in slot 0 or not.

To upgrade a system with two Routing Engines, refer to Figure 8 on page 119 and perform the following steps:

Figure 8: Upgrading to the 64-bit Junos OS with Dual Routing Engines

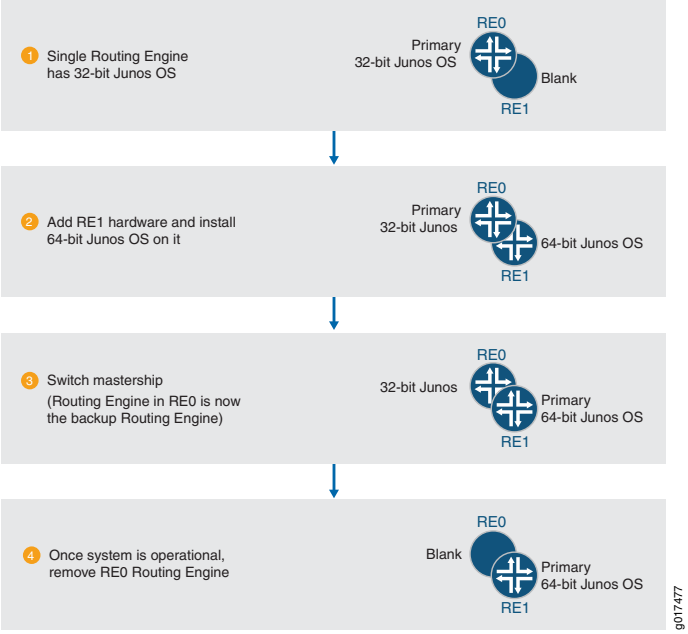


1. In the initial state, both Routing Engines are running the 32-bit Junos OS, and slot 0 has the master Routing Engine.
2. Upgrade the slot 1 Routing Engine hardware and install the 64-bit Junos OS.

   For instructions on replacing a Routing Engine, see the hardware guide for your router.
3. Switch the master Routing Engine from slot 0 to slot 1 (allow the 32-bit Junos OS to co-exist with the 64-bit Junos OS).
4. Upgrade the slot 0 routing engine hardware and install the 64-bit Junos OS.
5. Both Routing Engines now run the 64-bit Junos OS. Optionally, you can switch the master Routing Engine back to slot 0.

NOTE: Mixing the 32-bit Junos OS with the 64-bit Junos OS is only supported temporarily during the upgrade process. Mixing the two operating systems is not supported for normal operations.

Figure 9: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master in Either Slot)



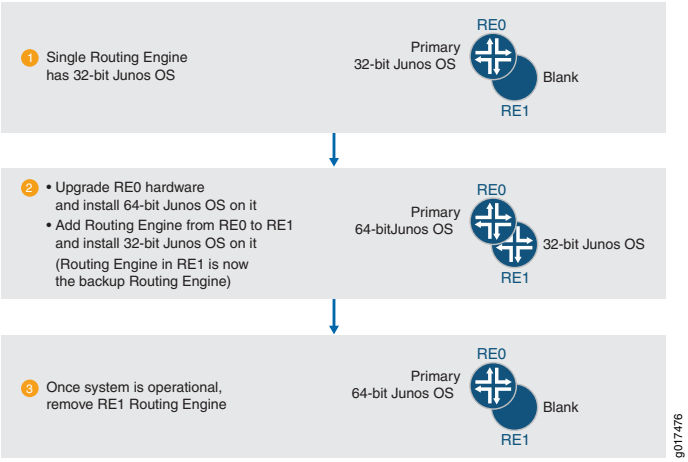
To upgrade a system with a single Routing Engine, where the master Routing Engine can be in either slot 0 or slot 1, refer to Figure 8 on page 119and perform the following steps:

1. In the initial state, the slot 0 Routing Engine is running the 32-bit Junos OS and slot 1 is blank.
2. Install the upgraded Routing Engine hardware in slot 1 and install the 64-bit Junos OS.

   For instructions on installing a Routing Engine, see the hardware guide for your router.
3. When the 64-bit Junos OS is configured properly, remove the slot 0 Routing Engine running the 32-bit Junos OS.

To upgrade a system with a single Routing Engine, where the master Routing Engine must be in slot 0, refer to Figure 10 on page 121 and perform the following steps:

Figure 10: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master Must Be in Slot 0)



1. In the initial state, the slot 0 Routing Engine is running the 32-bit Junos OS and slot 1 is blank.
2. Install the slot 0 Routing Engine hardware in slot 1. Install the upgraded Routing Engine hardware in slot 0 and install the 64-bit Junos OS.

   For instructions on installing a Routing Engine, see the hardware guide for your router.
3. When the 64-bit Junos OS is configured properly, remove the slot 1 routing engine running the 32-bit Junos OS.

Related Documentation

- Checklist for Reinstalling Junos OS on page 251

Upgrading Routers Using ISSU

Unified in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic. ISSU is only supported by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled.

For additional information about using ISSU, see the *Junos OS High Availability Library for Routing Devices*.

For additional information about using ISSU on SRX Series devices, see the *Junos OS High Availability Guide*.

Understanding Nonstop Software Upgrade on EX Series Switches

Nonstop software upgrade (NSSU) enables you to upgrade the software running on Juniper Networks EX Series Ethernet Switches with redundant Routing Engines and all

member switches in EX Series Virtual Chassis by using a single command and with minimal network traffic disruption during the upgrade.

NSSU is supported on the following platforms:

- EX3300 Virtual Chassis
- EX4200 Virtual Chassis
- EX4300 Virtual Chassis
- EX4500 Virtual Chassis
- EX4550 Virtual Chassis
- All mixed Virtual Chassis composed of EX4200, EX4500, and EX4550 switches
- EX6200 switches
- EX8200 switches
- EX8200 Virtual Chassis

Performing an NSSU provides these benefits:

- No disruption to the control plane—An NSSU takes advantage of graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) to ensure no disruption to the control plane. During the upgrade process, interface, kernel, and routing protocol information is preserved.
- Minimal disruption to network traffic—An NSSU minimizes network traffic disruption by:
  - Upgrading line cards one at a time in an EX6200 switch, EX8200 switch, or EX8200 Virtual Chassis, permitting traffic to continue to flow through the line cards that are not being upgraded.
  - Upgrading member switches one at a time in an EX3300, EX4200, EX4300, EX4500, or mixed Virtual Chassis, permitting traffic to continue to flow through the members that are not being upgraded.

  To achieve minimal disruption to traffic, you must configure link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards or Virtual Chassis members. When one member link of a LAG is down, the remaining links are up, and traffic continues to flow through the LAG.

NOTE: Because NSSU upgrades the software on each line card or on each Virtual Chassis member one at a time, an upgrade using NSSU can take longer than an upgrade using the **request system software add** command.

For EX6200 switches, EX8200 switches, and EX8200 Virtual Chassis, you can reduce the amount of time an upgrade takes by configuring line-card upgrade groups. The line cards in an upgrade group are upgraded simultaneously, reducing the amount of time it takes to complete an upgrade. See "Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)" on page 145.

This topic covers:

Requirements for Performing an NSSU

The following requirements apply to all switches and Virtual Chassis:

- All Virtual Chassis members and all Routing Engines must be running the same Junos OS release.
- Graceful Routing Engine switchover (GRES) must be enabled.
- Nonstop active routing (NSR) must be enabled.

  NOTE: Although nonstop bridging (NSB) does not have to be enabled to perform an NSSU, we recommend enabling NSB before performing an NSSU. Enabling NSB ensures that all NSB-supported Layer 2 protocols operate seamlessly during the Routing Engine switchover that is part of the NSSU. See *Configuring Nonstop Bridging on EX Series Switches (CLI Procedure)*.

- For minimal traffic disruption, you must define link aggregation groups (LAGs) such that the member links reside on different Virtual Chassis members or on different line cards.

The following are requirements for EX3300, EX4200, EX4300, EX4500, and mixed Virtual Chassis:

- The Virtual Chassis members must be connected in a ring topology so that no member is isolated as a result of another member being rebooted. This topology prevents the Virtual Chassis from splitting during an NSSU.
- The Virtual Chassis master and backup must be adjacent to each other in the ring topology. Adjacency permits the master and backup to always be in sync, even when the switches in linecard roles are rebooting.
- The Virtual Chassis must be preprovisioned so that the linecard role has been explicitly assigned to member switches acting in a linecard role. During an NSSU, the Virtual Chassis members must maintain their roles—the master and backup must maintain their master and backup roles (although mastership will change), and the remaining switches must maintain their linecard roles.
- A two-member Virtual Chassis must have **no-split-detection** configured so that the Virtual Chassis does not split when an NSSU upgrades a member.

NOTE: For the EX4300 Virtual Chassis, you should enable the **vcp-no-hold-time** statement at the **[edit virtual-chassis]** hierarchy level before performing a software upgrade using NSSU. If you do not enable the **vcp-no-hold-time** statement, the Virtual Chassis may split during the upgrade. A split Virtual Chassis can cause disruptions to your network, and you may have to manually reconfigure your Virtual Chassis after the NSSU if the split and merge feature was disabled. For more information about a split Virtual Chassis, see *Understanding Split and Merge in a Virtual Chassis*

How an NSSU Works

This section describes what happens when you request an NSSU on these switches and Virtual Chassis:

- EX3300, EX4200, EX4300, EX4500, and Mixed Virtual Chassis on page 124
- EX6200 and EX8200 Switches on page 125
- EX8200 Virtual Chassis on page 126

EX3300, EX4200, EX4300, EX4500, and Mixed Virtual Chassis

When you request an NSSU on an EX3300, EX4200, EX4300, EX4500, or mixed Virtual Chassis:

1. The Virtual Chassis master verifies that:
   - The backup is online and running the same software version.
   - Graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) are enabled.
   - The Virtual Chassis has a preprovisioned configuration.
2. The master installs the new software image on the backup and reboots it.
3. The master resynchronizes the backup.

4. The master installs the new software image on member switches that are in the linecard role and reboots them, one at a time. The master waits for each member to become online and active before starting the software upgrade on the next member.
5. When all members that are in the linecard role have been upgraded, the master performs a graceful Routing Engine switchover, and the upgraded backup becomes the master.
6. The software on the original master is upgraded and the original master is automatically rebooted. After the original master has rejoined the Virtual Chassis, you can optionally return control to it by requesting a graceful Routing Engine switchover.

EX6200 and EX8200 Switches

When you request an NSSU on a standalone switch with redundant Routing Engines:

1. The switch verifies that:
   - Both Routing Engines are online and running the same software version.
   - Both Routing Engines have sufficient storage space for the new software image.
   - Graceful Routing Engine switchover and nonstop active routing are enabled.
2. The switch installs the new software image on the backup Routing Engine and reboots it.
3. The switch resynchronizes the backup Routing Engine to the master Routing Engine.
4. The line cards in the first upgrade group (or the line card in slot 0, if no upgrade groups are defined) download the new image and then restart. Traffic continues to flow through the line cards in the other upgrade groups during this process.
5. When line cards restarted in Step 4 are online again, the line cards in the next upgrade group download the new image and restart. This process continues until all online line cards have restarted with the new software.

   NOTE: **If you have taken a line card offline with the CLI before you start the NSSU, the line card is not restarted and remains offline.**

6. The switch performs a graceful Routing Engine switchover, so that the upgraded backup Routing Engine becomes the master.
7. The switch installs the new software on the original master Routing Engine.

   To complete the upgrade process, the original master Routing Engine must be rebooted. You can do so manually or have the switch perform an automatic reboot by including the **reboot** option when you request the NSSU. After the original master has been rebooted, you can optionally return control to it by requesting a graceful Routing Engine switchover.
8. (EX6200 switch only) The original master Routing Engine reboots to complete the software upgrade.

NOTE: To complete the upgrade process on an EX8200 switch, you must intervene to reboot the original master Routing Engine. You can reboot the original master Routing Engine manually or have the switch perform an automatic reboot by including the reboot option when you request the NSSU.

9. (Optional) After the original master has been rebooted, you can return control to it by requesting a graceful Routing Engine switchover.

   The switch can maintain normal operations with either Routing Engine acting as the master Routing Engine after the software upgrade, so you only have to perform this switchover if you want to return Routing Engine control to the original master Routing Engine.

EX8200 Virtual Chassis

When you request an NSSU on an EX8200 Virtual Chassis:

1. The master external Routing Engine verifies that:
   - It has a backup external Routing Engine that is online.
   - All Virtual Chassis members have redundant Routing Engines and the Routing Engines are online.
   - All Routing Engines are running the same software version.
   - All Routing Engines have sufficient storage space for the new software image.
   - Graceful Routing Engine switchover and nonstop active routing (NSR) are enabled.
2. The master external Routing Engine installs the new software image on the backup external Routing Engine and reboots it.
3. The backup external Routing Engine resynchronizes with the master external Routing Engine.
4. The master external Routing Engine installs the new software on the backup Routing Engines in the member switches and reboots the backup Routing Engines.
5. When the reboot of the backup Routing Engines complete, the line cards in the first upgrade group download the new image and then restart. (If no upgrade groups are defined, the line card in slot 0 of member 0 downloads the new image and restarts.) Traffic continues to flow through the line cards in the other upgrade groups during this process.
6. When line cards restarted in Step 5 are online again, the line cards in the next upgrade group (or the next sequential line card) download the new image and restart. This process continues until all online line cards have restarted with the new software.

   NOTE: If you have taken a line card offline with the CLI before you start the NSSU, the line card is not restarted and remains offline.

7. The new software image is installed on the master Routing Engines, both external and internal.
8. The member switches perform a graceful Routing Engine switchover, so that the upgraded backup Routing Engines become masters.
9. The master external Routing Engine performs a graceful Routing Engine switchover so that the backup external Routing Engine is now the master.

To complete the upgrade process, the original master Routing Engines, both external and internal, must be rebooted. You can do so manually by establishing a console connection to each Routing Engine or have the reboot performed automatically by including the **reboot** option when you request the NSSU. After the original master external Routing Engine has been rebooted, you can optionally return control to it by requesting a graceful Routing Engine switchover.

NSSU Limitations

You cannot use an NSSU to downgrade the software—that is, to install an earlier version of the software than is currently running on the switch. To install an earlier software version, use the **request system software add** command.

You cannot roll back to the previous software version after you perform an upgrade using NSSU. If you need to rollback to the previous software version, you can do so by rebooting from the alternate root partition if you have not already copied the new software version into the alternate root partition.

NSSU and Junos OS Release Support

A Virtual Chassis must be running a Junos OS release that supports NSSU before you can perform an NSSU. If a Virtual Chassis is running a software version that does not support NSSU, use the **request system software add** command.

Table 19 on page 127 lists the EX Series switches and Virtual Chassis that support NSSU and the Junos OS release at which they began supporting it.

Table 19: Platform and Release Support for NSSU

Platform	Junos OS Release
EX3300 Virtual Chassis	12.2 or later
EX4200 Virtual Chassis	12.1 or later
EX4300 Virtual Chassis	13.2X51-D20 or later
EX4500 Virtual Chassis	12.1 or later
EX4550 Virtual Chassis	12.2 or later
Mixed EX4200 and EX4500 Virtual Chassis	12.1 or later
Mixed EX4200 and EX4550 Virtual Chassis	12.2 or later

Table 19: Platform and Release Support for NSSU *(continued)*

Platform	Junos OS Release
Mixed EX4200, EX4500, and EX4550 Virtual Chassis	12.2 or later
Mixed EX4500 and EX4550 Virtual Chassis	12.2 or later
EX6200 switch	12.2 or later
EX8200 switch	10.4 or later
EX8200 Virtual Chassis	11.1 or later

Overview of NSSU Configuration and Operation

You must ensure that the configuration of the switch or Virtual Chassis meets the requirements described in "Requirements for Performing an NSSU" on page 123. NSSU requires no additional configuration.

For EX6200 switches, EX8200 switches, and EX8200 Virtual Chassis, you can optionally configure line-card upgrade groups using the CLI. See "Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches" on page 147.

You perform an NSSU by executing the **request system software nonstop-upgrade** command. For detailed instructions on how to perform an NSSU, see the topics in Related Documentation.

Related Documentation

- Upgrading Software on an EX3300, EX4200, EX4300, EX4500 and EX4550 Virtual Chassis, and Mixed Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure) on page 128
- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) on page 132
- Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure) on page 140
- *Configuring Nonstop Active Routing on Switches*
- *Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure)*
- Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches on page 147

Upgrading Software on an EX3300, EX4200, EX4300, EX4500 and EX4550 Virtual Chassis, and Mixed Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)

You can use nonstop software upgrade (NSSU) to upgrade the software running on all member switches in most EX Series Virtual Chassis with minimal traffic disruption during the upgrade.

NSSU is supported on the following Virtual Chassis platforms:

- EX3300 Virtual Chassis
- EX4200 Virtual Chassis
- EX4300 Virtual Chassis
- EX4500 Virtual Chassis
- EX4550 Virtual Chassis
- All mixed Virtual Chassis composed of EX4200, EX4500, and EX4550 switches
- EX8200 Virtual Chassis

This topic covers:

- Preparing the Switch for Software Installation on page 129
- Upgrading the Software Using NSSU on page 130

Preparing the Switch for Software Installation

Before you begin software installation using NSSU:

- Ensure that the Virtual Chassis is configured correctly to support NSSU. Verify that:
  - The Virtual Chassis members are connected in a ring topology. A ring topology prevents the Virtual Chassis from splitting during an NSSU.
  - The Virtual Chassis master and backup are adjacent to each other in the ring topology. Adjacency permits the master and backup to always be in sync, even when the switches in linecard roles are rebooting.
  - The Virtual Chassis is preprovisioned so that the linecard role has been explicitly assigned to member switches acting in the linecard role. During an NSSU, the Virtual Chassis members must maintain their roles—the master and backup must maintain their master and backup roles (although mastership will change), and the other member switches must maintain their linecard roles.

    For information on configuring a preprovisioned Virtual Chassis, see *Configuring an EX3300 Virtual Chassis (CLI Procedure)*, *Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)*, and *Configuring an EX8200 Virtual Chassis (CLI Procedure)*.
  - A two-member Virtual Chassis has **no-split-detection** configured so that the Virtual Chassis does not split when an NSSU upgrades a member.
- Verify that the members are running the same version of the software:

  user@switch> **show version**

  If the Virtual Chassis members are not running the same version of the software, use the **request system software add** command to upgrade the software on the inconsistent members.
- Ensure that nonstop active routing (NSR) and graceful Routing Engine switchover (GRES) are enabled. To verify that they are enabled, you need to check only the state

of nonstop active routing—if nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

To verify that nonstop active routing is enabled:

```
user@switch> show task replication
        Stateful Replication: Enabled
        RE mode: Master

    Protocol                Synchronization Status
    OSPF                    Complete
    BGP                     Complete
    PIM                     Complete
```

If nonstop active routing is not enabled (**Stateful Replication** is **Disabled**), see *Configuring Nonstop Active Routing on Switches* for information on how to enable it.

- For the EX4300 Virtual Chassis, you should enable the **vcp-no-hold-time** statement at the [**edit virtual-chassis**] hierarchy level before performing a software upgrade using NSSU. If you do not enable the **vcp-no-hold-time** statement, the Virtual Chassis may split during the upgrade. A split Virtual Chassis can cause disruptions to your network, and you may have to manually reconfigure your Virtual Chassis after the NSSU if the split and merge feature was disabled. For more information about a split Virtual Chassis, see *Understanding Split and Merge in a Virtual Chassis*
- (Optional) Enable nonstop bridging (NSB). Enabling NSB ensures that all NSB-supported Layer 2 protocols operate seamlessly during the Routing Engine switchover that is part of the NSSU.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on each member to an external storage device with the **request system snapshot** command.

Upgrading the Software Using NSSU

This procedure describes how to upgrade the software running on all Virtual Chassis members using NSSU. When the upgrade completes, all members are running the new version of the software. Because a graceful Routing Engine switchover occurs during the upgrade, the original Virtual Chassis backup is the new master.

To upgrade all members using NSSU:

1. Download the software package by following the procedure in "Downloading Software Packages from Juniper Networks" on page 42. If you are upgrading the software running on a mixed Virtual Chassis, download the software packages for both switch types.
2. Copy the software package or packages to the Virtual Chassis. We recommend that you copy the file to the **/var/tmp** directory on the master.
3. Log in to the Virtual Chassis using the console connection or the virtual management Ethernet (VME) interface. Using a console connection allows you to monitor the progress of the master switch reboot.
4. Start the NSSU:

- On an EX3300 Virtual Chassis, EX4200 Virtual Chassis, EX4300 Virtual Chassis, EX4500 Virtual Chassis, or EX4550 Virtual Chassis, enter:

  user@switch> **request system software nonstop-upgrade /var/tmp/*package-name*.tgz**

  where ***package-name*.tgz** is, for example, **jinstall-ex4200-12.1R2.5-domestic-signed.tgz**.

- On a mixed Virtual Chassis, enter:

  user@switch> **request system software nonstop-upgrade set [/var/tmp/*package-name*.tgz /var/tmp/*package-name*.tgz]**

  where **[/var/tmp/*package-name*.tgz /var/tmp/*package-name*.tgz]** specifies the EX4200 and EX4500 software packages.

The switch displays status messages similar to the following messages as the upgrade executes:

```
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Installing image on other FPC's along with the backup

Checking pending install on fpc1
Pushing bundle to fpc1
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
Completed install on fpc1

Checking pending install on fpc2
Pushing bundle to fpc2
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
Completed install on fpc2

Rebooting fpc1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online
  FPC 1          Online
  FPC 2          Online (ISSU)
Going to install image on master
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
relinquish mastership
ISSU: IDLE

*** FINAL System shutdown message from user@switch ***
```

```
System going down IMMEDIATELY


Shutdown NOW!
[pid 9336]
```

5. Log in after the reboot of the original master switch completes. To verify that the software on all Routing Engines in the Virtual Chassis members has been upgraded, enter the following command:

   user@switch> **show version**

6. To ensure that the resilient dual-root partitions feature operates correctly, copy the new Junos OS image into the alternate root partitions of all members:

   user@switch> **request system snapshot slice alternate all-members**

   Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Related Documentation

- Understanding Nonstop Software Upgrade on EX Series Switches on page 121
- Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure) on page 140
- Understanding Resilient Dual-Root Partitions on Switches on page 93
- Understanding Software Installation on EX Series Switches on page 35
- Troubleshooting Software Installation on page 321
- Junos OS Package Names on page 6
- Understanding Nonstop Software Upgrade on EX Series Switches on page 121

Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)

You can use nonstop software upgrade (NSSU) to upgrade the software on standalone EX6200 or EX8200 switches with redundant Routing Engines. NSSU upgrades the software running on the Routing Engines and line cards with minimal traffic disruption during the upgrade. NSSU is supported on EX8200 switches running Junos OS Release 10.4 or later and on EX6200 switches running Junos OS Release 12.2 or later.

This topic covers:

- Preparing the Switch for Software Installation on page 132
- Upgrading Both Routing Engines Using NSSU on page 134
- Upgrading One Routing Engine Using NSSU (EX8200 Switch Only) on page 137
- Upgrading the Original Master Routing Engine (EX8200 Switch Only) on page 139

Preparing the Switch for Software Installation

Before you begin software installation using NSSU:

- (Optional) Configure line-card upgrade groups as described in "Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)" on page 145. By default, an NSSU upgrades line cards one at a time to allow aggregated Ethernet links that have members on different line cards to remain up through the upgrade process. Configuring line-card upgrade groups reduces the time an upgrade takes because the line cards in each upgrade group are upgraded at the same time rather than sequentially.

- Verify that the Routing Engines are running the same version of the software. Enter the following command:

```
{master}
user@switch> show version invoke-on all-routing-engines
re0:
--------------------------------------------------------------------------
Hostname: switch
Model: ex8208
JUNOS Base OS boot [11.3-20110429.1]
JUNOS Base OS Software Suite [11.3-20110429.1]
JUNOS Kernel Software Suite [11.3-20110429.1]
JUNOS Crypto Software Suite [11.3-20110429.1]
JUNOS Online Documentation [11.3-20110429.1]
JUNOS Enterprise Software Suite [11.3-20110429.1]
LC JUNOS Installation Software [11.3-20110429.1]
JUNOS Routing Software Suite [11.3-20110429.1]
JUNOS Web Management [11.3-20110429.1]

re1:
--------------------------------------------------------------------------
Hostname: switch
Model: ex8208
JUNOS Base OS boot [11.3-20110429.1]
JUNOS Base OS Software Suite [11.3-20110429.1]
JUNOS Kernel Software Suite [11.3-20110429.1]
JUNOS Crypto Software Suite [11.3-20110429.1]
JUNOS Online Documentation [11.3-20110429.1]
JUNOS Enterprise Software Suite [11.3-20110429.1]
LC JUNOS Installation Software [11.3-20110429.1]
JUNOS Routing Software Suite [11.3-20110429.1]
JUNOS Web Management [11.3-20110429.1]
```

  If the Routing Engines are not running the same version of the software, use the **request system software add** command to upgrade the Routing Engine that is running the earlier software version. For instructions on upgrading a single Routing Engine, see "Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)" on page 59.

- Ensure that nonstop active routing (NSR) and graceful Routing Engine switchover (GRES) are enabled. To verify that they are enabled, you need to check only the state of nonstop active routing—if nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

  To verify that nonstop active routing is enabled, execute the following command:

```
{master}
user@switch> show task replication
        Stateful Replication: Enabled
        RE mode: Master
```

```
Protocol                Synchronization Status
OSPF                    Complete
RIP                     Complete
PIM                     Complete
RSVP                    Complete
```

If nonstop active routing is not enabled (**Stateful Replication** is **Disabled**), see *Configuring Nonstop Active Routing on Switches* for information on how to enable it.

- (Optional) Enable nonstop bridging (NSB). Enabling NSB ensures that all NSB-supported Layer 2 protocols operate seamlessly during the Routing Engine switchover that is part of the NSSU.
- (Optional) Back up the system software on each Routing Engine to an external storage device with the **request system snapshot** command.

Upgrading Both Routing Engines Using NSSU

This procedure describes how to upgrade both Routing Engines using NSSU. When the upgrade completes, both Routing Engines are running the new version of the software, and the backup Routing Engine is the new master Routing Engine.

To upgrade both Routing Engines using NSSU:

1. Download the software package by following the procedure in "Downloading Software Packages from Juniper Networks" on page 42.
2. Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.
3. Log in to the master Routing Engine using the console connection. You can perform an NSSU from the management interface, but a console connection allows you to monitor the progress of the master Routing Engine reboot.
4. Install the new software package:

   {master}
   user@switch> **request system software nonstop-upgrade reboot /var/tmp/*package-name-m.nZx-distribution*.tgz**

   where ***package-name-m.nZx-distribution*.tgz** is, for example, **jinstall-ex-8200-10.4R1.5-domestic-signed.tgz**.

   The switch displays the following status messages as the upgrade executes:

```
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Pushing bundle to re1
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
Backup upgrade done
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
```



```
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
  FPC 1          Online (ISSU)
  FPC 2          Online (ISSU)
  FPC 3          Offline                 Offlined by CLI command
  FPC 4          Online (ISSU)
  FPC 5          Online (ISSU)
  FPC 6          Online (ISSU)
  FPC 7          Online (ISSU)
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
ISSU: Upgrading Old Master RE
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
ISSU: Old Master Upgrade Done
ISSU: IDLE


*** FINAL System shutdown message from user@switch ***
System going down IMMEDIATELY

Shutdown NOW!
[pid 2635]
```

NOTE: If you omit the **reboot** option in this step when using an EX8200 switch, you must manually reboot the original master Routing Engine with the request system reboot command for the upgrade to complete.

The original master Routing Engine reboots automatically after updating the new master Routing Engine when an NSSU is used to upgrade an EX6200 switch with dual Routing Engines.

5. Log in after the reboot completes. To verify that both Routing Engines have been upgraded, enter the following command:

```
{backup}
user@switch> show version invoke-on all-routing-engines
re0:
--------------------------------------------------------------------
Hostname: switch
Model: ex8208
JUNOS Base OS boot [12.1-20111229.0]
JUNOS Base OS Software Suite [12.1-20111229.0]
JUNOS Kernel Software Suite [12.1-20111229.0]
JUNOS Crypto Software Suite [12.1-20111229.0]
JUNOS Online Documentation [12.1-20111229.0]
JUNOS Enterprise Software Suite [12.1-20111229.0]
LC JUNOS Installation Software [12.1-20111229.0]
JUNOS Routing Software Suite [12.1-20111229.0]
JUNOS Web Management [12.1-20111229.0]
```

```
re1:
--------------------------------------------------------------------
Hostname: switch
Model: ex8208
JUNOS Base OS boot [12.1-20111229.0]
JUNOS Base OS Software Suite [12.1-20111229.0]
JUNOS Kernel Software Suite [12.1-20111229.0]
JUNOS Crypto Software Suite [12.1-20111229.0]
JUNOS Online Documentation [12.1-20111229.0]
JUNOS Enterprise Software Suite [12.1-20111229.0]
LC JUNOS Installation Software [12.1-20111229.0]
JUNOS Routing Software Suite [12.1-20111229.0]
JUNOS Web Management [12.1-20111229.0]
```

6. To verify that the line cards that were online before the upgrade are online after the upgrade, log in to the master Routing Engine and enter the **show chassis nonstop-upgrade** command:

```
{backup}
user@switch> request routing-engine login master

{master}
user@switch> show chassis nonstop-upgrade
  Item           Status                  Reason
  FPC 0          Online (ISSU)
  FPC 1          Online (ISSU)
  FPC 2          Online (ISSU)
  FPC 3          Offline                 Offlined by CLI command
  FPC 4          Online (ISSU)
  FPC 5          Online (ISSU)
  FPC 6          Online (ISSU)
  FPC 7          Online (ISSU)
```

7. If you want to make **re0** the master Routing Engine again, enter the following command:

```
{master}
user@switch> request chassis routing-engine master switch
Toggle mastership between routing engines ? [yes,no] (no) yes
```

   You can verify that **re0** is the master Routing Engine by executing the **show chassis routing-engine** command.

8. To ensure that the resilient dual-root partitions feature operates correctly, execute the following command to copy the new Junos OS image into the alternate root partition on each Routing Engine:

   user@switch> **request system snapshot slice alternate routing-engine both**

   Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Upgrading One Routing Engine Using NSSU (EX8200 Switch Only)

This procedure describes how to upgrade one of the Routing Engines using NSSU on an EX8200 switch. When the upgrade completes, the backup Routing Engine is running the new software version and is the new master. The original master Routing Engine, now the backup Routing Engine, continues to run the previous software version.

NOTE: **NSSU always upgrades the software on both Routing Engines on an EX6200 switch. Therefore, you cannot upgrade software on one Routing Engine using NSSU on an EX6200 switch.**

To upgrade one Routing Engine using NSSU:

1. Download the software package by following the procedure in "Downloading Software Packages from Juniper Networks" on page 42.
2. Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.
3. Log in to the master Routing Engine.
4. Request an NSSU. On an EX8200 switch, specify the **no-old-master-upgrade** option when requesting the NSSU:

   {master}
   user@switch> **request system software nonstop-upgrade no-old-master-upgrade /var/tmp/*package-name-m.nZx-distribution*.tgz**

   where ***package-name-m.nZx-distribution*.tgz** is, for example, **jinstall-ex-8200-10.4R2.5-domestic-signed.tgz**.

   The switch displays the following status messages as the upgrade executes:

```
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Pushing bundle to re1
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
Backup upgrade done
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
```

```
  FPC 1          Online (ISSU)
  FPC 2          Online (ISSU)
  FPC 3          Offline                Offlined by CLI command
  FPC 4          Online (ISSU)
  FPC 5          Online (ISSU)
  FPC 6          Online (ISSU)
  FPC 7          Online (ISSU)
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
Skipping Old Master Upgrade
ISSU: IDLE
```

When the upgrade is complete, the original master Routing Engine (**re0**) becomes the backup Routing Engine.

5. To verify that the original backup Routing Engine (**re1**) has been upgraded, enter the following command:

```
{backup}
user@switch> show version invoke-on all-routing-engines
re0:
--------------------------------------------------------------------------
Hostname: switch
Model: ex8208
JUNOS Base OS boot [11.3-20110429.1]
JUNOS Base OS Software Suite [11.3-20110429.1]
JUNOS Kernel Software Suite [11.3-20110429.1]
JUNOS Crypto Software Suite [11.3-20110429.1]
JUNOS Online Documentation [11.3-20110429.1]
JUNOS Enterprise Software Suite [11.3-20110429.1]
LC JUNOS Installation Software [11.3-20110429.1]
JUNOS Routing Software Suite [11.3-20110429.1]
JUNOS Web Management [11.3-20110429.1]

re1:
--------------------------------------------------------------------------
Hostname: switch
Model: ex8208
JUNOS Base OS boot [12.1-20111229.0]
JUNOS Base OS Software Suite [12.1-20111229.0]
JUNOS Kernel Software Suite [12.1-20111229.0]
JUNOS Crypto Software Suite [12.1-20111229.0]
JUNOS Online Documentation [12.1-20111229.0]
JUNOS Enterprise Software Suite [12.1-20111229.0]
LC JUNOS Installation Software [12.1-20111229.0]
JUNOS Routing Software Suite [12.1-20111229.0]
JUNOS Web Management [12.1-20111229.0]
```

6. To verify that the line cards that were online before the upgrade are online after the upgrade, log in to the new master Routing Engine and enter the **show chassis nonstop-upgrade** command:

```
{backup}
user@switch> request routing-engine login master

--- JUNOS 12.1-20111229.0 built 2011-12-29 04:12:22 UTC
{master}
user@switch> show chassis nonstop-upgrade
  Item           Status                 Reason
  FPC 0          Online
```

```
FPC 1          Online
FPC 2          Online
FPC 3          Offline                 Offlined by CLI command
FPC 4          Online
FPC 5          Online
FPC 6          Online
FPC 7          Online
```

7. To ensure that the resilient dual-root partitions feature operates correctly, copy the new Junos OS image into the alternate root partition of the Routing Engine:

   user@switch> **request system snapshot slice alternate**

   Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Upgrading the Original Master Routing Engine (EX8200 Switch Only)

This procedure describes how to upgrade the original master Routing Engine after you have upgraded the original backup Routing Engine as described in "Upgrading One Routing Engine Using NSSU (EX8200 Switch Only)" on page 137 for an EX8200 switch.

1. Log in to the current master Routing Engine (**re1**).
2. Enter configuration mode and disable nonstop active routing:

   {master}[edit]
   user@switch# **delete routing-options nonstop-routing**

3. Deactivate graceful Routing Engine switchover and commit the configuration:

   {master}[edit]
   user@switch# **deactivate chassis redundancy graceful-switchover**

   {master}[edit]
   user@switch# **commit**

4. Log in to the current backup Routing Engine (**re0**) using a console connection.
5. Request a software installation:

   user@switch> request system software add **reboot**
   /var/tmp/*package-name-m.nZx-distribution*.tgz

   NOTE: When you use NSSU to upgrade only one Routing Engine, the installation package is not automatically deleted from /var/tmp, leaving the package available to be used to upgrade the original master Routing Engine.

6. After the upgrade completes, log in to the current master Routing Engine (**re1**) and enter CLI configuration mode.
7. Re-enable nonstop active routing and graceful Routing Engine switchover:

   [edit]
   user@switch# **activate chassis redundancy graceful-switchover**

```
[edit]
user@switch# set routing-options nonstop-routing

[edit]
user@switch# commit
```

8. To ensure that the resilient dual-root partitions feature operates correctly, exit the CLI configuration mode and copy the new Junos OS image into the alternate root partition of the Routing Engine:

   ```
   user@switch> request system snapshot slice alternate
   ```

   Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

9. (Optional) To return control to the original master Routing Engine (**re0**), enter the following command:

   ```
   {master}
   user@switch> request chassis routing-engine master switch
    Toggle mastership between routing engines ? [yes,no] (no) yes
   ```

   You can verify that **re0** is the master Routing Engine by executing the **show chassis routing-engine** command.

Related Documentation

- Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches on page 147
- Understanding Resilient Dual-Root Partitions on Switches on page 93
- Troubleshooting Software Installation on page 321
- Junos OS Package Names on page 6
- Understanding Nonstop Software Upgrade on EX Series Switches on page 121
- Understanding Software Installation on EX Series Switches on page 35

Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)

You can use nonstop software upgrade (NSSU) to upgrade the software on an EX8200 Virtual Chassis. NSSU upgrades the software running on all Routing Engines with minimal traffic disruption during the upgrade. NSSU is supported on EX8200 Virtual Chassis with redundant XRE200 External Routing Engines running Junos OS Release 11.1 or later.

NOTE: NSSU upgrades all Routing Engines on all members of the Virtual Chassis and on the XRE200 External Routing Engines. Using NSSU, you cannot choose to upgrade the backup Routing Engines only, nor can you choose to upgrade a specific member of the Virtual Chassis. If you need to upgrade a specific member of the Virtual Chassis, see *Installing Software for a Single Device in an EX8200 Virtual Chassis*.

This topic covers:

- Preparing the Switch for Software Installation on page 141
- Upgrading the Software Using NSSU on page 142

Preparing the Switch for Software Installation

Before you begin software installation using NSSU:

- (Optional) Configure line-card upgrade groups as described in "Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)" on page 145. By default, NSSU upgrades line cards one at a time, starting with the line card in slot 0 of member 0. This permits aggregated Ethernet links that have members on different line cards remain up through the upgrade process. Configuring line-card upgrade groups reduces the time an upgrade takes because the line cards in each upgrade group are upgraded at the same time rather than sequentially.

- Verify that the members are running the same version of the software:

  ```
  {master:8}
  user@external-routing-engine> show version all-members
  ```

  If the Virtual Chassis members are not running the same version of the software, use the **request system software add** command to upgrade the software on the inconsistent members. For instructions, see *Installing Software for a Single Device in an EX8200 Virtual Chassis*.

- Ensure that nonstop active routing (NSR) and graceful Routing Engine switchover (GRES) are enabled. To verify that they are enabled, you need to check only the state of nonstop active routing—if nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

  To verify that nonstop active routing is enabled:

  ```
  {master:8}
  user@switch> show task replication
          Stateful Replication: Enabled
          RE mode: Master

      Protocol                Synchronization Status
          PIM                     Complete
  ```

  If nonstop active routing is not enabled (**Stateful Replication** is **Disabled**), see *Configuring Nonstop Active Routing on Switches* for information on how to enable it.

Upgrading the Software Using NSSU

This procedure describes how to upgrade the software running on all Routing Engines using NSSU. When the upgrade completes, all Routing Engines are running the new version of the software. The backup external Routing Engine is now the master external Routing Engine, and the internal backup Routing Engines in the member switches are now the internal master Routing Engines in those member switches.

To upgrade all Routing Engines using NSSU:

1. Download the software package for the XRE200 External Routing Engine by following the procedure in "Downloading Software Packages from Juniper Networks" on page 42. The name of the software package for the XRE200 External Routing Engine contains the term **xre200**.
2. Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.
3. Log in to the master external Routing Engine using the console connection. You can perform an NSSU from the management interface, but a console connection allows you to monitor the progress of the master Routing Engine reboot.
4. Install the new software package:

   {master:8}
   user@external-routing-engine> **request system software nonstop-upgrade reboot /var/tmp/*package-name-m.nZx-distribution*.tgz**

   where ***package-name-m.nZx-distribution*.tgz** is, for example, **jinstall-ex-xre200-11.1R2.5-domestic-signed.tgz**.

   NOTE: You can omit reboot option. When you include the reboot option, NSSU automatically reboots the original master Routing Engines after the new image has been installed on them. If you omit the reboot option, you must manually reboot the original master Routing Engines (now the backup Routing Engines) to complete the upgrade. To perform the reboot, you must establish a connection to the console port on the Switch Fabric and Routing Engine (SRE) module or Routing Engine (RE) module.

   The switch displays status messages similar to the following messages as the upgrade executes:

```
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing LCC Backup REs
ISSU: Preparing Backup RE
Pushing bundle /var/tmp/jinstall-ex-xre200-11.1-20110208.0-domestic-signed.tgz
 to member9
member9:
--------------------------------------------------------------------------
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
VC Backup upgrade done
Rebooting VC Backup RE
```

```
Rebooting member9
ISSU: Backup RE Prepare Done
Waiting for VC Backup RE reboot
Pushing bundle to member0-backup
Pushing bundle to member1-backup
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately

Rebooting member0-backup
Rebooting LCC [member0-backup]

Rebooting member1-backup
Rebooting LCC [member1-backup]
ISSU: LCC Backup REs Prepare Done
GRES operational
Initiating Chassis Nonstop-Software-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking Nonstop-Upgrade status
member0:
--------------------------------------------------------------------------
  Item           Status                  Reason
  FPC 0          Online (ISSU)
  FPC 1          Online (ISSU)
  FPC 2          Online (ISSU)
  FPC 5          Online (ISSU)

member1:
--------------------------------------------------------------------------
  Item           Status                  Reason
  FPC 0          Online (ISSU)
  FPC 1          Online (ISSU)
  FPC 2          Online (ISSU)
  FPC 5          Online (ISSU)

member0:
--------------------------------------------------------------------------
  Item           Status                  Reason
  FPC 0          Online (ISSU)
  FPC 1          Online (ISSU)
  FPC 2          Online (ISSU)
  FPC 5          Online (ISSU)

member1:
--------------------------------------------------------------------------
  Item           Status                  Reason
  FPC 0          Online (ISSU)
  FPC 1          Online (ISSU)
  FPC 2          Online (ISSU)
  FPC 5          Online (ISSU)
ISSU: Upgrading Old Master RE
Pushing bundle /var/tmp/incoming-package-8200.tgz to member0-master
Pushing bundle /var/tmp/incoming-package-8200.tgz to member1-master
ISSU: RE switchover Done
```

```
WARNING: A reboot is required to install the software
WARNING:     Use the 'request system reboot' command immediately
ISSU: Old Master Upgrade Done
ISSU: IDLE

*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY



Shutdown NOW!
```

NOTE: If you omit the **reboot** option in this step, you must complete the upgrade by separately rebooting the original master Routing Engine on each Virtual Chassis member and the original master external Routing Engine. To reboot the original master Routing Engine on a Virtual Chassis member, you must establish a connection to the console port on the Switch Fabric and Routing Engine (SRE) module or Routing Engine (RE) module.

5. Log in after the reboot completes. To verify that the software on all Routing Engines in the Virtual Chassis members has been upgraded, enter the following command:

```
{backup:8}
user@external-routing-engine> show version all-members
```

6. Verify that the line cards that were online before the upgrade are online after the upgrade by entering the **show chassis nonstop-upgrade** command:

```
{backup:8}
user@external-routing-engine> show chassis nonstop-upgrade
member0:
--------------------------------------------------------------------------
  Item           Status                  Reason
  FPC 0          Online
  FPC 1          Online
  FPC 2          Online
  FPC 5          Online

member1:
--------------------------------------------------------------------------
  Item           Status                  Reason
  FPC 0          Online
  FPC 1          Online
  FPC 2          Online
  FPC 5          Online
```

Related Documentation

- Upgrading Software on an EX3300, EX4200, EX4300, EX4500 and EX4550 Virtual Chassis, and Mixed Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure) on page 128
- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) on page 132
- Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches on page 147

- Understanding Resilient Dual-Root Partitions on Switches on page 93
- Troubleshooting Software Installation on page 321
- Junos OS Package Names on page 6
- Understanding Nonstop Software Upgrade on EX Series Switches on page 121
- Understanding Software Installation on EX Series Switches on page 35

Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)

Nonstop software upgrade (NSSU) enables you to upgrade the software running on an EX Series switch with redundant Routing Engines, on most EX Series Virtual Chassis, QFX3500, QFX3600, and QFX5100 Virtual Chassis, and Virtual Chassis Fabric by using a single command and with minimal disruption to network traffic.

In its default configuration, NSSU upgrades each line card in a switch or Virtual Chassis or Virtual Chassis Fabric one at a time. Traffic continues to flow through the other line cards while a line card is being restarted as part of the upgrade. This behavior allows you to minimize disruption to traffic by configuring link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards. When one member link of a LAG is down, the remaining links are up, and traffic continues to flow through the LAG.

To reduce the time an NSSU takes, you can configure line-card upgrade groups on an EX6200 or EX8200 switch with redundant Routing Engines, EX8200 Virtual Chassis, QFX3500, QFX3600, and QFX5100 Virtual Chassis, and Virtual Chassis Fabric.

NOTE: **NSSU line-card upgrade groups are not supported for NSSUs on EX3300 Virtual Chassis, EX4200 Virtual Chassis, EX4300 Virtual Chassis, EX4500 Virtual Chassis, EX4550 Virtual Chassis, or any mixed Virtual Chassis composed of EX4200, EX4500, or EX4550 switches.**

When you define an upgrade group, NSSU upgrades the line cards in the upgrade group at the same time instead of sequentially. To achieve minimal traffic disruption, you must define the line-card upgrade groups such that the member links of the LAGs reside on line cards that are in different upgrade groups. For information on how to configure LAGs, see *Configuring Aggregated Ethernet Links (CLI Procedure)*.

To configure line-card upgrade groups on a standalone EX6200 or EX8200 switch:

- To create an upgrade group and add a line card to it:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group group-name fpcs slot-number
  ```

  For example, to create an upgrade group called **group3** and add the line card in slot 5 to it:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group group3 fpcs 5
  ```

  If **group3** already exists, this command adds line card 5 to **group3**.

- To create an upgrade group and add multiple line cards to it:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group group-name fpcs (NSSU Upgrade Groups)
  [list-of-slot-numbers]
  ```

  For example, to create an upgrade group called **primary** and add line cards in slots 1, 4, and 7 to it:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group primary fpcs [1 4 7]
  ```

  If **primary** already exists, this command adds line cards in slots 1, 4, and 7 to **primary**.

To configure line-card upgrade groups on an EX8200 Virtual Chassis:

- To create an upgrade group and add a line card on a Virtual Chassis member to it:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group group-name member (NSSU Upgrade Groups) member-id
  fpcs slot-number
  ```

  For example, to create an upgrade group called **primary-ny** and add the line card on member 1 in slot 5 to it:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group primary-ny member 1 fpcs 5
  ```

  If **primary-ny** already exists, this command adds line card 5 on member 1 to **primary-ny**.

- To create an upgrade group that contains multiple line cards on a Virtual Chassis member:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group group-name member member-id fpcs
  [list-of-slot-numbers]
  ```

  For example, to create an upgrade group called **primary-ny** that contains the line cards in slots 1 and 2 on member 0 and in slots 3 and 4 on member 1:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group primary-ny member 0 fpcs [1 2]

  [edit chassis]
  user@switch# set nssu upgrade-group primary-ny member 1 fpcs [3 4]
  ```

To configure line-card upgrade groups on a Virtual Chassis Fabric:

- To create an upgrade group and add a line card member on a Virtual Chassis Fabric to the upgrade group:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group group-name primary fpcs value
  ```

  For example, to create an upgrade group called **vcf** and add a line card member:

  ```
  [edit chassis]
  user@switch# set nssu upgrade-group vcf primary fpcs 2
  ```

  If **vcf** already exists, this command adds line card 2 to **vcf**.

- To create an upgrade group that contains multiple line cards on a Virtual Chassis Fabric:


```
[edit chassis]
user@switch# set nssu upgrade-group group-name primary fpcs [list-of-slot-numbers]
```

For example, to create an upgrade group called **vcf** that contains line cards 1 and 2:

```
[edit chassis]
user@switch# set nssu upgrade-group vcf primary fpcs [1 2]
```

Related Documentation

- Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches on page 147
- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) on page 132
- Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure) on page 140
- *Upgrading Software on a Virtual Chassis Fabric Using Nonstop Software Upgrade*
- Understanding Nonstop Software Upgrade on EX Series Switches on page 121

Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches

Nonstop software upgrade (NSSU) enables you to upgrade the software running on an EX Series switch with redundant Routing Engines or on most EX Series Virtual Chassis by using a single command and with minimal disruption to network traffic. By default, NSSU upgrades the software running on line cards one line card at a time.

To reduce the time an NSSU takes, you can configure line-card upgrade groups on an EX6200 or EX8200 switch with redundant Routing Engines or on an EX8200 Virtual Chassis.

This example shows how to configure NSSU to use line-card upgrade groups:

Requirements

This example uses the following hardware and software components:

- An EX8200 switch with redundant Routing Engines
- Junos OS Release 10.4 or later for EX Series switches

Before you begin to configure line-card upgrade groups, ensure that you have configured the link aggregation groups (LAGs) as described in *Configuring Aggregated Ethernet Links (CLI Procedure)*. See "Overview and Topology" on page 148 for details about the LAG configurations for this example.

Overview and Topology

In its default configuration, NSSU upgrades each line card in a switch or Virtual Chassis one at a time. Traffic continues to flow through the other line cards while a line card is being restarted as part of the upgrade. This behavior allows you minimize disruption to traffic by configuring link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards. When one member link of a LAG is down, the remaining links are up, and traffic continues to flow through the LAG.

Because the default configuration upgrades each line card one at a time, the upgrade can take some time to complete. You can reduce the time it takes to perform an NSSU by configuring line-card upgrade groups. Instead of being upgraded sequentially, the line cards in an upgrade group are upgraded simultaneously. To achieve minimal traffic disruption, you must define the line-card upgrade groups such that the member links of the LAGs reside on line cards that are in different upgrade groups.

This example uses an EX8200 switch that has five line cards installed in slots 0 through 4. Two LAGs have been configured:

- **ae0**—Has two member links, one on the line card in slot 0 and one on the line card in slot 1.
- **ae1**—Has two member links, one on the line card in slot 2 and one on the line card in slot 3.

The interfaces on the line card in slot 4 are not part of either LAG.

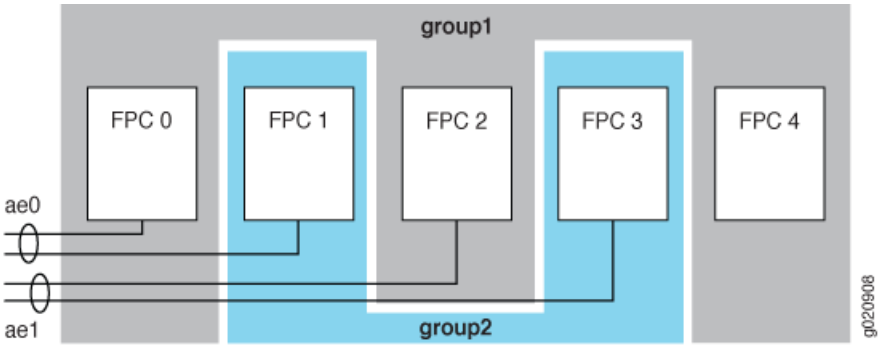
To minimize the time an upgrade takes and to ensure that the member links of each LAG are in different upgrade groups, this example configures the following two line-card upgrade groups:

- **group1**—Contains the line cards in slots 0, 2, and 4.
- **group2**—Contains the line cards in slots 1 and 3.

The line card in slot 4 could be put in either group. It could also be left out of an upgrade group entirely, and it would be upgraded separately after the line cards in the upgrade groups have been upgraded. However, it is more efficient to include it in an upgrade group.

Figure 11 on page 149 illustrates the topology.

Figure 11: Example Line-Card Upgrade Group Topology



Configuration

To create line-card upgrade groups, perform these tasks:

CLI Quick Configuration

To quickly create the line-card upgrade groups, copy the following commands and paste them into the switch terminal window:

```
[edit]
set chassis nssu upgrade-group group1 fpcs [0 2 4]
set chassis nssu upgrade-group group2 fpcs [1 3]
```

Step-by-Step Procedure

To create the line-card upgrade groups for an NSSU:

1. Create the first line-card upgrade group:

   ```
   [edit chassis]
   user@switch# set nssu upgrade-group group1 fpcs [0 2 4]
   ```

2. Create the second line-card upgrade group:

   ```
   [edit chassis]
   user@switch# set nssu upgrade-group group2 fpcs (NSSU Upgrade Groups) [1 3]
   ```

Results

Display the results of the configuration:

```
[edit chassis]
user@switch# show
nssu {
    upgrade-group group1 {
        fpcs [ 0 2 4 ];
    }
    upgrade-group group2 {
        fpcs [ 1 3 ];
    }
}
```

Related Documentation

- Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure) on page 145
- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) on page 132
- Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure) on page 140

Upgrading Software on a QFabric System

The QFabric system software package contains software for all of the different components in the QFabric system, such as the Director group, Interconnect devices, Node devices, and other QFabric system components. You can upgrade the software on all of the QFabric components at the same time using the **request system software add *package-name* component all reboot** command.

NOTE: Downgrading software on a QFabric system is not supported.

This topic describes the following tasks:

- Backing Up the Current Configuration Files on page 150
- Downloading Software Files Using a Browser on page 150
- Retrieving Software Files for Download on page 151
- Installing the Software Package on the Entire QFabric System on page 151

Backing Up the Current Configuration Files

To back up your current configuration files:

`user@switch>` **request system software configuration-backup *path***

Back up the configuration files to a local directory, remote server, or removable drive (for example, an external USB flash drive).

For example:

`user@switch>` **request system software configuration-backup /media/USB/**

Downloading Software Files Using a Browser

NOTE: To access the download site, you must have a service contract with Juniper Networks and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website https://www.juniper.net/registration/Register.jsp .

1. Using a Web browser, navigate to the http://www.juniper.net/support .
2. Click **Download Software**.
3. In the **Switching** box, click **Junos OS Platforms**.
4. In the **QFX Series** section, click the name of the platform for which you want to download software.
5. Click the **Software** tab and select the release number from the **Release** drop-down list.
6. Select the complete install package you want to download in the **QFabric System Install Package** section:

- If you want to upgrade the entire QFabric system, select **QFabric System - Complete Install Package**.
- If you want to upgrade either a single Node or Interconnect device for recovery purposes, select **Node and Interconnect Device Install Package**. For information on how to perform a recovery installation on either a Node or Interconnect device, see "Performing a Recovery Installation" on page 227.

A login screen appears.

7. Enter your user ID and password and click **Login**.
8. Read the End User License Agreement, select the **I agree** option button, and then click **Proceed**.
9. Save the **jinstall-qfabric-*version*.rpm** file on your computer.

Retrieving Software Files for Download

Retrieve the software from the location in which you downloaded it. To do this, issue the **request system software download** command. The software package is copied from where you downloaded it and is placed locally on the QFabric system.

- To retrieve the software:

  `user@switch>` **request system software download */path/package-name***

  For example:

  `user@switch>` **request system software download ftp://server/files/jinstall-qfabric-11.3X30.6.rpm**

Installing the Software Package on the Entire QFabric System

NOTE: On a QFabric system, a QFX3500 Node device or QFX3600 Node device might not be able to participate as a Node device in the QFabric system if the Node device is running a different version of software from that of the Director group. This mismatch of software versions between the Node device and the Director group can occur when the Node device is introduced into the setup, and both Director devices go offline before the Node device completes its auto-upgrade process to upgrade its software version to the same software version running on the Director group. The workaround is to reboot the QFX3500 or QFX3600 Node device once the Director group comes back online. The QFX3500 or QFX3600 Node device will initiate auto-upgrade and upgrade its software version from the Director group.

1. Issue the **request system software add *package-name* component all reboot** command.

   For example:

   `user@switch>` **request system software add jinstall-qfabric-11.3X30.6.rpm component all reboot**

NOTE: If you receive an error message after issuing the **request system software add *package-name* component all reboot** command that says that the configuration file cannot be loaded as is, you will need to enter configuration mode, make any necessary changes to the configuration file, and then commit the changes.

NOTE: The default value for a QFabric system software upgrade is **validate**. The validation step adds up to 10 minutes to the overall software upgrade. If the validation fails, the upgrade does not proceed and the QFabric system automatically issues the **request system software rollback** command to restore the current software image. If you upgrade more than one component (for example, by issuing the **component all** option), validation failure on one device stops the upgrade process for the other devices. If you do not want to validate the software package against the current configuration, issue the **no-validate** option.

2. After the reboot has finished, verify that the new version of software has been properly installed by issuing the **show version component all** command.

```
user@switch> show version component all
dg1:
-
Hostname: qfabric
Model: qfx3100
JUNOS Base Version [11.3X30.6]

dg0:
-
Hostname: qfabric
Model: qfx3100
JUNOS Base Version [11.3X30.6]

NW-NG-0:
-
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

FC-0:
-
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
```

```
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

FC-1:
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

DRE-0:
-
Hostname: dre-0
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

FM-0:
-
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

nodedevice1:
-
Hostname: qfabric
Model: QFX3500
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

interconnectdevice1:
-
Hostname: qfabric
Model: QFX3108
JUNOS Base OS boot [11.3X30.6]
```

```
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]
```

Related Documentation

- *Software Installation Overview*
- Performing a QFabric System Recovery Installation on the Director Group on page 229
- *Upgrading Jloader Software on QFX Series Devices*
- **request system software add on page 373**
- *Installation and Upgrade Guide*

Understanding Nonstop Software Upgrade for QFabric Systems

The framework that underlies a nonstop software upgrade in a QFabric system enables you to upgrade the system in a step-by-step manner and minimize the impact to the continuous operation of the system. This topic explains how a nonstop software upgrade works in a QFabric system, the steps that are involved, and the procedures that you need to implement to experience the benefits of this style of software upgrade.

Nonstop software upgrade enables some QFabric system components to continue operating while similar components in the system are being upgraded. In general, the QFabric system upgrades redundant components in stages so that some components remain operational and continue forwarding traffic while their equivalent counterparts upgrade to a new version of software.

TIP: Use the following guidelines to decide when to implement a nonstop software upgrade:

TIP: Before you perform a nonstop software upgrade, contact JTAC to perform a pre-upgrade health check on the QFabric system.

- If you need to upgrade all components of the system in the shortest amount of time (approximately one hour) and you do not need to retain the forwarding resiliency of the data plane, issue the **request system software add component all** command to perform a standard software upgrade. All components of the QFabric system upgrade simultaneously and expediently, but this type of upgrade does not provide resiliency or switchover capabilities.
- If you need to minimize service impact, preserve the forwarding operations of the data plane during the upgrade, and are willing to take the extra time required for component switchovers (in many cases, several hours), issue the three nonstop software upgrade commands (**request system software**

nonstop-upgrade (director-group | fabric | node-group) described in this topic in the correct order.

NOTE:

- Before you begin a nonstop software upgrade, issue the **request system software download** command to copy the software to the QFabric system.
- Each of the 3 nonstop software upgrade steps must be considered parts of the whole process. You must complete all 3 steps of a nonstop software upgrade in the correct order to ensure the proper operation of the QFabric system.
- Open two SSH sessions to the QFabric CLI. Use one session to monitor the upgrade itself and use a second session to verify that the QFabric system components respond to operational mode commands as expected. For more information on verification of the upgrade, see "Verifying Nonstop Software Upgrade for QFabric Systems" on page 158.
- Issue the **show fabric administration inventory** command to verify that all upgraded components are operational at the end of a step before beginning the next step.
- Once you start the nonstop software upgrade process, we strongly recommend that you complete all 3 steps within 12 hours.

The three steps to a successful nonstop software upgrade must be performed in the following order:

- Director group—The first step upgrades the Director devices, the fabric manager Routing Engine, and the diagnostic Routing Engine. To perform the first step, issue the **request system software nonstop-upgrade director-group** command. The key actions that occur during a Director group upgrade are:
  1. Connecting to the QFabric system by way of an SSH connection. This action establishes a load-balanced CLI session on one of the Director devices in the Director group.
  2. The QFabric system downloads and installs the new software in both Director devices.
  3. The Director device hosting the CLI session becomes the master for all QFabric system processes running on the Director group, such as the fabric manager and network Node group Routing Engines.
  4. The QFabric system installs the new software for the backup fabric manager Routing Engine on the backup Director device.
  5. The backup Director device reboots to activate the new software.

6. The master Director device begins a 15 minute sequence that includes a temporary suspension of QFabric services and a QFabric database transfer. You cannot issue operational mode commands in the QFabric CLI during this period.
7. The QFabric system installs the new software for the fabric manager and diagnostic Routing Engines on the Director group master.
8. The QFabric system switches mastership of all QFabric processes from the master Director device to the backup Director device.
9. The master Director device reboots to activate the new software.
10. The CLI session terminates, and logging back in to the QFabric system with a new SSH connection establishes the session on the new master Director device (the original backup).
11. The previous master Director device resumes operation as a backup and the associated processes (such as the fabric manager and network Node group Routing Engines) become backup as well. The fabric control Routing Engine associated with this Director device returns to active status.

NOTE: After the Director group nonstop software upgrade completes, any Interconnect device or Node device that reboots will automatically download the new software, install it, and reboot again. As a result, try not to restart any QFabric system devices before you complete the rest of the nonstop software upgrade steps.

TIP:

- To enable BGP and OSPF to continue operating on the network Node group during a Director group nonstop service upgrade, we recommend that you configure graceful restart for these routing protocols. For more information on graceful restart, see *Configuring Graceful Restart for QFabric Systems*.
- Wait 15 minutes after the second Director device returns to service and hosts Routing Engine processes before proceeding to step 2—the fabric upgrade. You can verify the operational status of both Director devices by issuing the **show fabric administration inventory director-group status** command. Also, issue the **show fabric administration inventory infrastructure** command to verify when the Routing Engine processes become load balanced (typically, there will be three to four Routing Engines running on each Director device).

- Fabric—The second step upgrades the Interconnect devices and the fabric control Routing Engines. To perform the second step, issue the **request system software nonstop-upgrade fabric** command. The key actions that occur during a fabric upgrade are:

1. The QFabric system downloads, validates, and installs the new software in all Interconnect devices and fabric control Routing Engines (FC-0 and FC-1).
2. One fabric control Routing Engine reboots and comes back online.
3. The other fabric control Routing Engine reboots and comes back online.
4. The first Interconnect device reboots, comes back online, and resumes the forwarding of traffic.
5. Subsequent Interconnect devices reboot one at a time, come back online, and return to service.

NOTE:

- If the software does not load properly on any one of the fabric components, all components revert back to the original software version.
- If one of the components in a fabric upgrade does not reboot successfully, issue the **request system reboot fabric** command to reattempt the rebooting process for this fabric component and activate the new software.

- Node group—The third and final step upgrades Node groups. You can choose to upgrade a network Node group, a redundant server Node group, or individual server Node groups. You can upgrade the Node groups one at a time or in groups (known as upgrade groups). However, you must upgrade all Node groups in your QFabric system before you can complete the nonstop software upgrade process. To perform the third step, issue the **request system software nonstop-upgrade node-group** command.

  The key actions that occur during a network Node group upgrade are:

  1. The QFabric system copies the new software to each Node device one at a time.
  2. The QFabric system validates and then installs the new software in all Node devices simultaneously.
  3. The system copies the software to the network Node group Routing Engines.
  4. The QFabric system validates and then installs the software in the network Node group Routing Engines one at a time -- first the backup, then the master.
  5. The backup network Node group Routing Engine reboots and comes back online.
  6. The supporting Node devices reboot and come back online one at a time.

     NOTE: To reduce the total upgrade duration, configure an upgrade group. All Node devices within the upgrade group reboot at the same time.

  7. The master network Node group Routing Engine relinquishes mastership to the backup, reboots, and comes back online.

  The key actions that occur during a redundant server Node group upgrade are:

1. The QFabric system copies the new software to the backup Node device, then the master Node device.
2. The QFabric system validates and then installs the new software on the backup Node device, then the master Node device.
3. The backup Node device reboots, comes back online, and becomes the master Node device.
4. The previous master Node device reboots and comes back online as a backup Node device.

NOTE: For redundant server Node groups, both Node devices must be online before the upgrade will proceed. If one of the devices is no longer available, remove the Node device from the Node group configuration before you issue the nonstop software upgrade command.

The key actions that occur during a server Node group upgrade for a Node group that contains one member are:

1. The Node device downloads the software package and validates the software.
2. The Node device installs the software and reboots.

NOTE: Because there is no redundancy for Node groups containing a single Node device, traffic loss occurs when the device reboots during the upgrade.

Related Documentation

- *Nonstop Software Upgrade Checklist for QFabric Systems*
- *Performing a Nonstop Software Upgrade on the QFabric System*
- Verifying Nonstop Software Upgrade for QFabric Systems on page 158
- **request system software nonstop-upgrade on page 389**
- **request system software add on page 373**
- *Configuring Graceful Restart for QFabric Systems*

Verifying Nonstop Software Upgrade for QFabric Systems

NOTE: Before you perform a nonstop software upgrade, contact JTAC to perform a pre-upgrade health check on the QFabric system.

This topic discusses how you can monitor the progress of each of the three steps in a nonstop software upgrade. By identifying the key actions and events that define this process, you can track the status of the upgrade with confidence.

TIP: When performing a nonstop software upgrade, open two SSH sessions to the QFabric CLI. Use one session to monitor the upgrade itself and use a second session to verify that the QFabric system components respond to operational mode commands as expected.

- Verifying a Director Group Nonstop Software Upgrade on page 159
- Verifying a Fabric Nonstop Software Upgrade on page 172
- Verifying a Redundant Server Node Group Nonstop Software Upgrade on page 173
- Verifying a Network Node Group Nonstop Software Upgrade on page 176

Verifying a Director Group Nonstop Software Upgrade

Purpose During the Director group portion of a nonstop software upgrade, you should expect to see the Director device that hosts the CLI session selected as the master device. When mastership of all processes moves to the master, the QFabric system upgrades the backup Director device and this Director device reboots. After the backup Director device comes back online, the master Director device suspends CLI operations for 15 minutes, upgrades itself, and reboots. At this point, the backup becomes the new master Director device and you can issue CLI operational commands. Finally, the former master comes back online as a backup and both devices are operational once again. In addition to the steps below, you can issue the **show system software upgrade status** command to view the progress of the upgrade.

Action

1. In one SSH session to the QFabric CLI, verify the current status of the QFabric system by issuing the **show fabric administration inventory**, **show fabric administration inventory director-group status**, and **show fabric session-host** commands. In this case, Director device DG0 is the master device but DG1 hosts the CLI session.

```
session1@qfabric>  show fabric administration inventory
Item                    Identifier              Connection      Configuration
Node group
  NW-NG-0                                       Connected       Configured

    P1507-C                                     Connected

  RSNG                                          Connected       Configured

    P1550-C                                     Connected

    P1571-C                                     Connected

Interconnect device
  IC-F4912                                      Connected       Configured

    F4912/RE0                                   Connected

Fabric manager
  FM-0                                          Connected       Configured

Fabric control
  FC-0                                          Connected       Configured
```

```
  FC-1                                          Connected       Configured

Diagnostic routing engine
  DRE-0                                         Connected       Configured
```

session1@qfabric> show fabric administration inventory director-group status

```
Director Group Status Tue Jun  5 15:11:26 UTC 2012

 Member Status Role     Mgmt Address    CPU Free Memory VMs Up Time
 ------ ------ -------- --------------- --- ----------- --- -------------
 dg0    online master   10.49.215.38    8%  17363152k   4   3 days, 20:55 hrs

 dg1    online backup   10.49.215.39    6%  20157440k   3   3 days, 20:55 hrs


 Member Device Id/Alias  Status  Role
 ------ ---------------- ------- ---------
 dg0    0281052011000001 online  master

  Master Services
  ---------------
  Database Server                online
  Load Balancer Director         online
  QFabric Partition Address      online

  Director Group Managed Services
  -------------------------------
  Shared File System             online
  Network File System            online
  Virtual Machine Server         online
  Load Balancer/DHCP             online

  Hard Drive Status
  ----------------
  Volume ID:4                    optimal
  Physical ID:1                  online
  Physical ID:0                  online
  SCSI ID:1                      100%
  SCSI ID:0                      100%


  Size  Used Avail Used% Mounted on
  ----  ---- ----- ----- ----------
  423G 5.4G 395G  2%   /
  99M  16M  79M   17%  /boot
  93G  7.3G 86G   8%   /pbdata

  Director Group Processes
  ------------------------
  Director Group Manager         online
  Partition Manager              online
  Software Mirroring             online
  Shared File System master      online
  Secure Shell Process           online
  Network File System            online
  DHCP Server master             online     master

  FTP Server                     online
  Syslog                         online
  Distributed Management         online
  SNMP Trap Forwarder            online
```

```
 SNMP Process                   online
 Platform Management            online

 Interface Link Status
 ---------------------
 Management Interface           up
 Control Plane Bridge           up
 Control Plane LAG              up
 CP Link [0/2]                  up
 CP Link [0/1]                  up
 CP Link [0/0]                  up
 CP Link [1/2]                  down
 CP Link [1/1]                  down
 CP Link [1/0]                  down
 Crossover LAG                  up
 CP Link [0/3]                  up
 CP Link [1/3]                  up

Member Device Id/Alias  Status  Role
------ ---------------- ------- ---------
dg1    0281052011000032 online  backup

 Director Group Managed Services
 -------------------------------
 Shared File System             online
 Network File System            online
 Virtual Machine Server         online
 Load Balancer/DHCP             online

 Hard Drive Status
 ----------------
 Volume ID:8                    optimal
 Physical ID:1                  online
 Physical ID:0                  online
 SCSI ID:1                      100%
 SCSI ID:0                      100%


 Size  Used Avail Used% Mounted on
 ----  ---- ----- ----- ----------
 423G 5.5G 395G  2%   /
 99M  16M  79M   17%  /boot
 93G  7.3G 86G   8%   /pbdata

 Director Group Processes
 ------------------------
 Director Group Manager         online
 Partition Manager              online
 Software Mirroring             online
 Shared File System master      online
 Secure Shell Process           online
 Network File System            online
 DHCP Server master             online     backup

 FTP Server                     online
 Syslog                         online
 Distributed Management         online
 SNMP Trap Forwarder            online
 SNMP Process                   online
 Platform Management            online
```

```
Interface Link Status
---------------------
Management Interface           up
Control Plane Bridge           up
Control Plane LAG              up
CP Link [0/2]                  up
CP Link [0/1]                  up
CP Link [0/0]                  up
CP Link [1/2]                  down
CP Link [1/1]                  down
CP Link [1/0]                  down
Crossover LAG                  up
CP Link [0/3]                  up
CP Link [1/3]                  up
```

session1@qfabric> show fabric session-host

```
Identifier: 0281052011000032
```

2. In a second SSH session to the QFabric CLI, issue the request for the Director group nonstop software upgrade.

   root@qfabric> request system software nonstop-upgrade director-group jinstall-qfabric-12.2X50-D10.3.rpm

3. If the CLI session is being hosted by the master Director device, skip to step 4. However, if the CLI session is hosted by the backup Director device, the Director group mastership switches to the backup device after you issue the nonstop software upgrade command. In this example, mastership switches to Director device DG1.

   session1@qfabric> show fabric administration inventory director-group status

```
Director Group Status Tue Jun  5 15:12:20 UTC 2012

Member Status Role     Mgmt Address    CPU Free Memory VMs Up Time
------ ------ -------- --------------- --- ----------- --- -------------
dg0    online backup   10.49.215.38    8%  31905924k   0   3 days, 21:16 hrs

dg1    online master   10.49.215.39    6%  18010368k   3   3 days, 21:16 hrs


Member Device Id/Alias  Status  Role
------ ---------------- ------- ---------
dg0    0281052011000001 online  backup

 Director Group Managed Services
 -------------------------------
 Shared File System            offline
 Network File System           offline
 Virtual Machine Server        offline
 Load Balancer/DHCP            offline

 Hard Drive Status
 ----------------
 Volume ID:4                   optimal
 Physical ID:1                 online
 Physical ID:0                 online
 SCSI ID:1                     100%
 SCSI ID:0                     100%


 Size  Used Avail Used% Mounted on
 ----  ---- ----- ----- ----------
 423G 5.4G 395G  2%   /
```

```
 99M  16M  79M   17%  /boot

 Director Group Processes
 ------------------------
 Director Group Manager         online
 Partition Manager              online
 Software Mirroring             online
 Shared File System master      online
 Secure Shell Process           online
 Network File System            offline
 DHCP Server master             offline    backup

 FTP Server                     online
 Syslog                         online
 Distributed Management         offline
 SNMP Trap Forwarder            offline
 SNMP Process                   offline
 Platform Management            online

 Interface Link Status
 ---------------------
 Management Interface           up
 Control Plane Bridge           up
 Control Plane LAG              up
 CP Link [0/2]                  up
 CP Link [0/1]                  up
 CP Link [0/0]                  up
 CP Link [1/2]                  down
 CP Link [1/1]                  down
 CP Link [1/0]                  down
 Crossover LAG                  up
 CP Link [0/3]                  up
 CP Link [1/3]                  up

Member Device Id/Alias  Status  Role
------ ---------------- ------- ---------
dg1    0281052011000032 online  master

 Master Services
 ---------------
 Database Server                online
 Load Balancer Director         online
 QFabric Partition Address      online

 Director Group Managed Services
 -------------------------------
 Shared File System             online
 Network File System            online
 Virtual Machine Server         online
 Load Balancer/DHCP             online

 Hard Drive Status
 -----------------
 Volume ID:8                    optimal
 Physical ID:1                  online
 Physical ID:0                  online
 SCSI ID:1                      100%
 SCSI ID:0                      100%


 Size  Used Avail Used% Mounted on
```

```
----  ---- ----- ----- ----------
423G 6.0G 395G  2%   /
99M  16M  79M   17%  /boot
93G  7.3G 86G   8%   /pbdata

Director Group Processes
------------------------
Director Group Manager         online
Partition Manager              online
Software Mirroring             online
Shared File System master      online
Secure Shell Process           online
Network File System            online
DHCP Server master             online     master

FTP Server                     online
Syslog                         online
Distributed Management         online
SNMP Trap Forwarder            online
SNMP Process                   online
Platform Management            online

Interface Link Status
---------------------
Management Interface           up
Control Plane Bridge           up
Control Plane LAG              up
CP Link [0/2]                  up
CP Link [0/1]                  up
CP Link [0/0]                  up
CP Link [1/2]                  down
CP Link [1/1]                  down
CP Link [1/0]                  down
Crossover LAG                  up
CP Link [0/3]                  up
CP Link [1/3]                  up
```

session1@qfabric> show fabric session-host

```
Identifier: 0281052011000032
```

4. The Director group nonstop software upgrade process continues by downloading and installing software for the fabric manager Routing Engines and the Director devices.

root@qfabric>

```
Validating update package jinstall-qfabric-12.2X50-D10.3.rpm
Installing update package jinstall-qfabric-12.2X50-D10.3.rpm
Installing fabric images version 12.2X50-D10.3
Performing cleanup
Package install complete
Installing update package jinstall-qfabric-12.2X50-D10.3.rpm on peer
Triggering Initial Stage of Fabric Manager Upgrade
Updating CCIF default image to 12.2X50-D10.3
Updating FM-0 to Junos version 12.2X50-D10.3
[Status   2012-06-05 15:25:29]: Fabric Manager: Upgrade Initial Stage started
[FM-0     2012-06-05 15:25:38]: FM-0 Master already running on LOCAL DG
[NW-NG-0  2012-06-05 15:25:45]: NW-NG-0 Master already running on LOCAL DG
[FM-0     2012-06-05 15:26:12]: Retrieving package
[FM-0     2012-06-05 15:27:11]: Pushing bundle to re0
[Status   2012-06-05 15:29:06]: Load completed with 0 errors...
[Status   2012-06-05 15:29:06]: Reboot is required to complete upgrade ...
[Status   2012-06-05 15:29:07]: Trying to Connect to Node: FM-0
[Status   2012-06-05 15:29:13]: Rebooting FM-0
```



```
[FM-0     2012-06-05 15:29:13]: Waiting for FM-0 to terminate ...
Starting Peer upgrade

Initiating rolling upgrade of Director peer:  version 12.2X50-D10.3

Inform CCIF regarding rolling upgrade
[Peer Update Status]: Validating install package
jinstall-qfabric-12.2X50-D10.3.rpm
[Peer Update Status]: Cleaning up node for rolling phase one upgrade
[Peer Update Status]: Director group upgrade complete
[Peer Update Status]: COMPLETED
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
 upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase
 one of rolling upgrade
[Peer Update Status]: Waiting for peer to complete phase one of rolling upgrade
[Peer Update Status]: Peer completed phase one of rolling upgrade
```

5. When the system upgrades and reboots the backup Director device DG0, notice how this device is not displayed in the output of the **show fabric administration inventory director-group status** command. Because Director device DG1 appears, this means that the DG1 is operational and acts as the master device.

NOTE: If your second SSH session is being hosted by the rebooting Director device, your session terminates and you need to log back in to establish a new session running on the active Director device.

```
session1@qfabric>  show fabric administration inventory director-group status
Director Group Status Tue Jun  5 15:41:14 UTC 2012

 Member Status Role     Mgmt Address    CPU Free Memory VMs Up Time
 ------ ------ -------- --------------- --- ----------- --- -------------
 dg1    online master   10.49.215.39    6%  8372272k    4   3 days, 21:25 hrs


 Member Device Id/Alias  Status  Role
 ------ ---------------- ------- ---------
 dg1    0281052011000032 online  master

  Master Services
  ---------------
  Database Server                online
  Load Balancer Director         online
  QFabric Partition Address      online

  Director Group Managed Services
  -------------------------------
  Shared File System             online
  Network File System            online
  Virtual Machine Server         online
  Load Balancer/DHCP             online

  Hard Drive Status
  -----------------
  Volume ID:8                    optimal
  Physical ID:1                  online
  Physical ID:0                  online
  SCSI ID:1                      100%
  SCSI ID:0                      100%


  Size  Used Avail Used% Mounted on
  ----  ---- ----- ----- ----------
  423G 6.0G 395G  2%   /
  99M  16M  79M   17%  /boot
  93G  7.3G 86G   8%   /pbdata

  Director Group Processes
  ------------------------
  Director Group Manager         online
  Partition Manager              online
  Software Mirroring             online
  Shared File System master      online
  Secure Shell Process           online
  Network File System            online
  DHCP Server master             online     master

  FTP Server                     online
  Syslog                         online
  Distributed Management         online
```

```
  SNMP Trap Forwarder            online
  SNMP Process                   online
  Platform Management            online

  Interface Link Status
  ---------------------
  Management Interface           up
  Control Plane Bridge           up
  Control Plane LAG              up
  CP Link [0/2]                  up
  CP Link [0/1]                  up
  CP Link [0/0]                  up
  CP Link [1/2]                  down
  CP Link [1/1]                  down
  CP Link [1/0]                  down
  Crossover LAG                  up
  CP Link [0/3]                  up
  CP Link [1/3]                  up
```

6. The upgrade continues with master Director device DG1 suspending CLI services for 15 minutes, transferring mastership to Director device DG0, and then rebooting Director device DG1 (which terminates the CLI session).

```
root@qfabric>
[Peer Update Status]: Setting peer DG node as the master SFC

Delaying start of local upgrade to allow peer services time to initialize [15
 minutes]
Delaying start of local upgrade to allow peer services time to initialize [15
 minutes]
Delaying start of local upgrade to allow peer services time to initialize [12
 minutes]
Delaying start of local upgrade to allow peer services time to initialize [9
minutes]
Delaying start of local upgrade to allow peer services time to initialize [6
minutes]
Delaying start of local upgrade to allow peer services time to initialize [3
minutes]
[Peer Update Status]: Check for VMs on dg0
Triggering Final Stage of Fabric Manager Upgrade:
Updating FM-0 to Junos version 12.2X50-D10.3
[Status   2012-06-05 16:10:12]: Fabric Manager: Upgrade Final Stage started
[NW-NG-0  2012-06-05 16:10:22]: Transferring NW-NG-0 Mastership to REMOTE DG
[NW-NG-0  2012-06-05 16:11:44]: Finished NW-NG-0 Mastership switch
[Status   2012-06-05 16:11:45]: Upgrading FM-0 VM on worker DG to 12.2X50-D10.3
[DRE-0    2012-06-05 16:12:43]: Retrieving package
[DRE-0    2012-06-05 16:13:46]: ------- re0: -------
[Status   2012-06-05 16:15:17]: Load completed with 0 errors...
[Status   2012-06-05 16:15:17]: Reboot is required to complete upgrade ...
[DRE-0    2012-06-05 16:15:22]: Waiting for DRE-0 to terminate ...
[DRE-0    2012-06-05 16:15:34]: Waiting for DRE-0 to come back ...
[DRE-0    2012-06-05 16:18:44]: Running Uptime Test for DRE-0
[DRE-0    2012-06-05 16:18:51]: Uptime Test for DRE-0 Passed ...
[Status   2012-06-05 16:18:51]: DRE-0 booted successfully ...
Performing post install shutdown and cleanup

Broadcast message from root (Tue Jun  5 16:18:51 2012):

The system is going down for reboot NOW!
Director group upgrade complete
```

```
root@qfabric> Read from remote host qfabric-partition0: Connection reset by
peer
Connection to qfabric-partition0 closed.
```

7. Upon reopening the SSH session, notice that Director device DG0 is now the master device hosting the session and Director device DG1 does not appear in the QFabric system inventory while it is rebooting.

```
session1@qfabric>  show fabric session-host
Identifier: 0281052011000001

session1@qfabric>  show fabric administration inventory director-group status
Director Group Status Tue Jun  5 16:21:23 UTC 2012

 Member Status Role     Mgmt Address    CPU Free Memory VMs Up Time
 ------ ------ -------- --------------- --- ----------- --- -------------
 dg0    online master   10.49.215.38    13% 20739560k   3   36:29 mins


 Member Device Id/Alias  Status  Role
 ------ ---------------- ------- ---------
 dg0    0281052011000001 online  master

  Master Services
  ---------------
  Database Server                online
  Load Balancer Director         online
  QFabric Partition Address      online

  Director Group Managed Services
  -------------------------------
  Shared File System             online
  Network File System            online
  Virtual Machine Server         online
  Load Balancer/DHCP             online

  Hard Drive Status
  ----------------
  Volume ID:4                    optimal
  Physical ID:1                  online
  Physical ID:0                  online
  SCSI ID:1                      100%
  SCSI ID:0                      100%


  Size  Used Avail Used% Mounted on
  ----  ---- ----- ----- ----------
  423G 5.3G 396G  2%   /
  99M  16M  79M   17%  /boot
  93G  7.4G 86G   8%   /pbdata

  Director Group Processes
  ------------------------
  Director Group Manager         online
  Partition Manager              online
  Software Mirroring             online
  Shared File System master      online
  Secure Shell Process           online
  Network File System            online
  DHCP Server master             online     master

  FTP Server                     online
```



```
Syslog                          online
Distributed Management          online
SNMP Trap Forwarder             online
SNMP Process                    online
Platform Management             online

Interface Link Status
---------------------
Management Interface            up
Control Plane Bridge            up
Control Plane LAG               up
CP Link [0/2]                   up
CP Link [0/1]                   up
CP Link [0/0]                   up
CP Link [1/2]                   down
CP Link [1/1]                   down
CP Link [1/0]                   down
Crossover LAG                   up
CP Link [0/3]                   up
CP Link [1/3]                   up
```

8. When Director device DG1 comes back online, it returns to the QFabric system inventory as a backup Director device and hosts some of the Routing Engine processes (which should appear load balanced between the master and backup Director devices).

session1@qfabric> show fabric administration inventory director-group status

```
root@qfabric> show fabric administration inventory director-group status
Director Group Status Tue Jun  5 16:41:02 UTC 2012

Member Status Role     Mgmt Address    CPU Free Memory VMs Up Time
------ ------ -------- --------------- --- ----------- --- -------------
dg0    online master   10.49.215.38    15% 14759920k   6   56:09 mins

dg1    online backup   10.49.215.39    8%  31486680k   0   07:51 mins


Member Device Id/Alias  Status  Role
------ ---------------- ------- ---------
dg0    0281052011000001 online  master

 Master Services
 ---------------
 Database Server                online
 Load Balancer Director         online
 QFabric Partition Address      online

 Director Group Managed Services
 -------------------------------
 Shared File System             online
 Network File System            online
 Virtual Machine Server         online
 Load Balancer/DHCP             online

 Hard Drive Status
 -----------------
 Volume ID:4                    optimal
 Physical ID:1                  online
 Physical ID:0                  online
 SCSI ID:1                      100%
 SCSI ID:0                      100%
```

```
 Size  Used Avail Used% Mounted on
 ----  ---- ----- ----- ----------
 423G 5.3G 396G  2%   /
 99M  16M  79M   17%  /boot
 93G  7.4G 86G   8%   /pbdata

 Director Group Processes
 ------------------------
 Director Group Manager         online
 Partition Manager              online
 Software Mirroring             online
 Shared File System master      online
 Secure Shell Process           online
 Network File System            online
 DHCP Server master             online     master

 FTP Server                     online
 Syslog                         online
 Distributed Management         online
 SNMP Trap Forwarder            online
 SNMP Process                   online
 Platform Management            online

 Interface Link Status
 ---------------------
 Management Interface           up
 Control Plane Bridge           up
 Control Plane LAG              up
 CP Link [0/2]                  up
 CP Link [0/1]                  up
 CP Link [0/0]                  up
 CP Link [1/2]                  down
 CP Link [1/1]                  down
 CP Link [1/0]                  down
 Crossover LAG                  up
 CP Link [0/3]                  up
 CP Link [1/3]                  up

Member Device Id/Alias  Status  Role
------ ---------------- ------- ---------
dg1    0281052011000032 online  backup

 Director Group Managed Services
 -------------------------------
 Shared File System             online
 Network File System            online
 Virtual Machine Server         online
 Load Balancer/DHCP             online

 Hard Drive Status
 -----------------
 Volume ID:8                    optimal
 Physical ID:1                  online
 Physical ID:0                  online
 SCSI ID:1                      100%
 SCSI ID:0                      100%


 Size  Used Avail Used% Mounted on
```

```
  ----  ---- ----- ----- ----------
  423G 5.3G 396G  2%   /
  99M  16M  79M   17%  /boot
  93G  7.4G 86G   8%   /pbdata

  Director Group Processes
  ------------------------
  Director Group Manager         online
  Partition Manager              online
  Software Mirroring             online
  Shared File System master      online
  Secure Shell Process           online
  Network File System            online
  DHCP Server master             online     backup

  FTP Server                     online
  Syslog                         online
  Distributed Management         online
  SNMP Trap Forwarder            online
  SNMP Process                   online
  Platform Management            online

  Interface Link Status
  ---------------------
  Management Interface           up
  Control Plane Bridge           up
  Control Plane LAG              up
  CP Link [0/2]                  up
  CP Link [0/1]                  up
  CP Link [0/0]                  up
  CP Link [1/2]                  down
  CP Link [1/1]                  down
  CP Link [1/0]                  down
  Crossover LAG                  up
  CP Link [0/3]                  up
  CP Link [1/3]                  up
```

session1@qfabric> show fabric administration inventory infrastructure

```
dg0:
   Routing Engine Type                    Hostname              PID
CPU-Use(%)
------------------------- --------------------------------- ----------
-------------
 Fabric control              QFabric_default_FC-1_RE0         27906       2.5

 Network Node group          QFabric_default_NW-NG-1_RE1      20421       1.8

 Fabric manager              FM-0                             4211        1.8

 Debug Routing Engine        QFabric_DRE                      1575        3.3

dg1:
   Routing Engine Type                    Hostname              PID
CPU-Use(%)
------------------------- --------------------------------- ----------
-------------
 Fabric control              QFabric_default_FC-0_RE0         5686        2.3

 Network Node group          QFabric_default_NW-NG-0_RE0      5866        1.9

 Fabric manager              FM-1                             572         1.6
```

Verifying a Fabric Nonstop Software Upgrade

Purpose During the fabric portion of a nonstop software upgrade, you should expect to see both fabric control Routing Engines upgrade first, followed by the upgrade of each Interconnect device one at a time. In addition to the steps below, you can issue the **show system software upgrade status** command to view the progress of the upgrade.

Action

1. In an SSH session to the QFabric CLI, issue the request for the fabric nonstop software upgrade.

```
root@qfabric>  request system software nonstop-upgrade fabric
jinstall-qfabric-12.2X50-D10.3.rpm
[FC-0     2012-06-05 16:48:53]: Retrieving package
[FC-1     2012-06-05 16:48:53]: Retrieving package
[IC-F4912 2012-06-05 16:48:59]: Retrieving package
[FC-0     2012-06-05 16:49:51]: ------- re0: -------
[FC-1     2012-06-05 16:49:52]: ------- re0: -------
[IC-F4912 2012-06-05 16:49:54]: ------- re0: -------
[IC-F4912 2012-06-05 16:50:42]: Step 1 of 20 Creating temporary file system
[IC-F4912 2012-06-05 16:50:42]: Step 2 of 20 Determining installation source
[IC-F4912 2012-06-05 16:50:43]: Step 3 of 20 Processing format options
[IC-F4912 2012-06-05 16:50:43]: Step 4 of 20 Determining installation slice
[IC-F4912 2012-06-05 16:50:43]: Step 5 of 20 Creating and labeling new slices
[IC-F4912 2012-06-05 16:50:44]: Step 6 of 20 Create and mount new file system
[IC-F4912 2012-06-05 16:50:53]: Step 7 of 20 Getting OS bundles
[IC-F4912 2012-06-05 16:50:53]: Step 8 of 20 Updating recovery media
[IC-F4912 2012-06-05 16:51:17]: Step 9 of 20 Extracting incoming image
[IC-F4912 2012-06-05 16:52:56]: Step 10 of 20 Unpacking OS packages
[IC-F4912 2012-06-05 16:52:59]: Step 11 of 20 Mounting jbase package
[IC-F4912 2012-06-05 16:53:28]: Step 12 of 20 Creating base OS symbolic links
[IC-F4912 2012-06-05 16:54:45]: Step 13 of 20 Creating fstab
[IC-F4912 2012-06-05 16:54:45]: Step 14 of 20 Creating new system files
[IC-F4912 2012-06-05 16:54:46]: Step 15 of 20 Adding jbundle package
[IC-F4912 2012-06-05 16:58:15]: Step 16 of 20 Backing up system data
[IC-F4912 2012-06-05 16:58:18]: Step 17 of 20 Setting up shared partition data
[IC-F4912 2012-06-05 16:58:18]: Step 18 of 20 Checking package sanity in
installation
[IC-F4912 2012-06-05 16:58:18]: Step 19 of 20 Unmounting and cleaning up
temporary file systems
[IC-F4912 2012-06-05 16:58:22]: Step 20 of 20 Setting da0s1 as new active
partition
[Status   2012-06-05 16:58:34]: Load completed with 0 errors...
[Status   2012-06-05 16:58:34]: Reboot is required to complete upgrade ...
[Status   2012-06-05 16:58:34]: Trying to Connect to Node: FC-0
[Status   2012-06-05 16:58:39]: Rebooting FC-0
[Status   2012-06-05 16:58:39]: Trying to Connect to Node: FC-1
[Status   2012-06-05 16:58:44]: Rebooting FC-1
[Status   2012-06-05 16:58:44]: Trying to Connect to Node: IC-F4912
[Status   2012-06-05 16:58:50]: Rebooting IC-F4912
Success
```

2. When the fabric components reboot, they appear as **Disconnected** in the output of the **show fabric administration inventory infrastructure fabric-controls** and **show fabric administration inventory interconnect-devices** commands.

```
session1@qfabric>  show fabric administration inventory infrastructure fabric-controls
Item                    Identifier              Connection      Configuration
Fabric control
```



```
  FC-0                                          Disconnected
  FC-1                                          Disconnected
```

```
session1@qfabric>  show fabric administration inventory interconnect-devices IC-F4912
Item                    Identifier              Connection      Configuration
Interconnect device
  IC-F4912                                      Disconnected
    F4912/RE0                                   Disconnected
```

3. When the fabric components return to full service, they appear as **Connected** in the output of the **show fabric administration inventory** command.

```
session1@qfabric>  show fabric administration inventory
Item                    Identifier              Connection      Configuration
Node group
  NW-NG-0                                       Connected       Configured

    P1507-C                                     Connected

  RSNG                                          Connected       Configured

    P1550-C                                     Connected

    P1571-C                                     Connected

Interconnect device
  IC-F4912                                      Connected       Configured

    F4912/RE0                                   Connected

Fabric manager
  FM-0                                          Connected       Configured

Fabric control
  FC-0                                          Connected       Configured

  FC-1                                          Connected       Configured

Diagnostic routing engine
  DRE-0                                         Connected       Configured
```

Verifying a Redundant Server Node Group Nonstop Software Upgrade

Purpose During the redundant server Node group portion of a nonstop software upgrade, you should expect to see the backup Node device upgrade first, followed by the upgrade of the master Node device. Server Node groups with a single device upgrade the device in the same way as a standalone switch. In addition to the steps below, you can issue the **show system software upgrade status** command to view the progress of the upgrade.

Action

1. In an SSH session to the QFabric CLI, issue the request for the redundant server Node group nonstop software upgrade.

```
root@qfabric>  request system software nonstop-upgrade node-group RSNG
jinstall-qfabric-12.2X50-D10.3.rpm
Upgrading target(s): RSNG

[RSNG     2012-06-05 17:26:44]: Starting with package
ftp://169.254.0.3/pub/images/12.2X50-D10.3/jinstall-qfx.tgz
```

```
[RSNG     2012-06-05 17:26:44]: Retrieving package
[RSNG     2012-06-05 17:28:56]: Pushing bundle to fpc1
[RSNG     2012-06-05 17:29:26]: fpc1: Validate package...
[RSNG     2012-06-05 17:35:22]: fpc0: Validate package...
[RSNG     2012-06-05 17:35:49]: ------- fpc1 -------
[RSNG     2012-06-05 17:36:25]: Step 1 of 20 Creating temporary file system
[RSNG     2012-06-05 17:36:26]: Step 2 of 20 Determining installation source
[RSNG     2012-06-05 17:36:26]: Step 3 of 20 Processing format options
[RSNG     2012-06-05 17:36:26]: Step 4 of 20 Determining installation slice
[RSNG     2012-06-05 17:36:27]: Step 5 of 20 Creating and labeling new slices
[RSNG     2012-06-05 17:36:27]: Step 6 of 20 Create and mount new file system
[RSNG     2012-06-05 17:36:35]: Step 7 of 20 Getting OS bundles
[RSNG     2012-06-05 17:36:35]: Step 8 of 20 Updating recovery media
[RSNG     2012-06-05 17:36:56]: Step 9 of 20 Extracting incoming image
[RSNG     2012-06-05 17:38:07]: Step 10 of 20 Unpacking OS packages
[RSNG     2012-06-05 17:38:16]: Step 11 of 20 Mounting jbase package
[RSNG     2012-06-05 17:38:41]: Step 12 of 20 Creating base OS symbolic links
[RSNG     2012-06-05 17:39:41]: Step 13 of 20 Creating fstab
[RSNG     2012-06-05 17:39:42]: Step 14 of 20 Creating new system files
[RSNG     2012-06-05 17:39:42]: Step 15 of 20 Adding jbundle package
[RSNG     2012-06-05 17:42:16]: Step 16 of 20 Backing up system data
[RSNG     2012-06-05 17:42:32]: Step 17 of 20 Setting up shared partition data
[RSNG     2012-06-05 17:42:33]: Step 18 of 20 Checking package sanity in
installation
[RSNG     2012-06-05 17:42:33]: Step 19 of 20 Unmounting and cleaning up
temporary file systems
[RSNG     2012-06-05 17:42:36]: Step 20 of 20 Setting da0s2 as new active
partition
[RSNG     2012-06-05 17:42:51]: ------- fpc0 - master -------
[RSNG     2012-06-05 17:42:51]: Step 1 of 20 Creating temporary file system
[RSNG     2012-06-05 17:42:51]: Step 2 of 20 Determining installation source
[RSNG     2012-06-05 17:42:51]: Step 3 of 20 Processing format options
[RSNG     2012-06-05 17:42:51]: Step 4 of 20 Determining installation slice
[RSNG     2012-06-05 17:42:51]: Step 5 of 20 Creating and labeling new slices
[RSNG     2012-06-05 17:42:51]: Step 6 of 20 Create and mount new file system
[RSNG     2012-06-05 17:42:51]: Step 7 of 20 Getting OS bundles
[RSNG     2012-06-05 17:42:51]: Step 8 of 20 Updating recovery media
[RSNG     2012-06-05 17:42:51]: Step 9 of 20 Extracting incoming image
[RSNG     2012-06-05 17:42:51]: Step 10 of 20 Unpacking OS packages
[RSNG     2012-06-05 17:42:51]: Step 11 of 20 Mounting jbase package
[RSNG     2012-06-05 17:42:51]: Step 12 of 20 Creating base OS symbolic links
[RSNG     2012-06-05 17:42:51]: Step 13 of 20 Creating fstab
[RSNG     2012-06-05 17:42:51]: Step 14 of 20 Creating new system files
[RSNG     2012-06-05 17:42:51]: Step 15 of 20 Adding jbundle package
[RSNG     2012-06-05 17:42:51]: Step 16 of 20 Backing up system data
[RSNG     2012-06-05 17:42:51]: Step 17 of 20 Setting up shared partition data
[RSNG     2012-06-05 17:42:51]: Step 18 of 20 Checking package sanity in
installation
[RSNG     2012-06-05 17:42:51]: Step 19 of 20 Unmounting and cleaning up
temporary file systems
[RSNG     2012-06-05 17:42:51]: Step 20 of 20 Setting da0s2 as new active
partition
[RSNG     2012-06-05 17:43:36]: Rebooting Backup RE
[RSNG     2012-06-05 17:43:36]: ------- Rebooting fpc1 -------
[RSNG     2012-06-05 17:50:12]: Initiating Chassis In-Service-Upgrade
[RSNG     2012-06-05 17:50:33]: Upgrading group: 0 fpc: 0
[RSNG     2012-06-05 17:52:38]: Upgrade complete for group:0
[RSNG     2012-06-05 17:52:38]: Upgrading group: 1 fpc: 1
[RSNG     2012-06-05 17:54:42]: Upgrade complete for group:1
[RSNG     2012-06-05 17:54:42]: Finished processing all upgrade groups, last
group :1
```

```
[RSNG     2012-06-05 17:54:48]: Preparing for Switchover
[RSNG     2012-06-05 17:55:38]: Switchover Completed
[Status   2012-06-05 17:55:41]: Upgrade completed with 0 errors
Success
```

2. Issue the **show system software upgrade status** command to view the status of the upgrade.

```
root@qfabric>  show system software upgrade status
Wed Jan 16 22:06:02 2013 Software nonstop upgrade on:
                          RSNG in progress
```

3. During the redundant server Node group upgrade, the backup Node device (in this case, P1571-C) is upgraded first and appears in the **Disconnected** state in the output of the **show fabric administration inventory** command.

```
session1@qfabric>  show fabric administration inventory
Item                    Identifier              Connection      Configuration
Node group
  NW-NG-0                                       Connected       Configured

    P1507-C                                     Connected

  RSNG                                          Connected       Configured

    P1550-C                                     Connected

    P1571-C                                     Disconnected
Interconnect device
  IC-F4912                                      Connected       Configured

    F4912/RE0                                   Connected

Fabric manager
  FM-0                                          Connected       Configured

Fabric control
  FC-0                                          Connected       Configured

  FC-1                                          Connected       Configured

Diagnostic routing engine
  DRE-0                                         Connected       Configured
```

4. After the backup Node device comes back online, the master Node device (in this case, P1550-C) appears in the **Disconnected** state in the output of the **show fabric administration inventory** command while the master Node device upgrades its software.

```
session1@qfabric>  show fabric administration inventory
Item                    Identifier              Connection      Configuration
Node group
  NW-NG-0                                       Connected       Configured

    P1507-C                                     Connected

  RSNG                                          Connected       Configured

    P1550-C                                     Disconnected
    P1571-C                                     Connected
```

```
Interconnect device
  IC-F4912                                        Connected       Configured

    F4912/RE0                                     Connected

Fabric manager
  FM-0                                            Connected       Configured

Fabric control
  FC-0                                            Connected       Configured

  FC-1                                            Connected       Configured

Diagnostic routing engine
  DRE-0                                           Connected       Configured
```

5. After both Node devices in the redundant server Node group come back online, both Node devices appear as **Connected** to indicate the successful completion of the Node group nonstop software upgrade step.

```
session1@qfabric>  show fabric administration inventory
Item                    Identifier              Connection      Configuration
Node group
  NW-NG-0                                         Connected       Configured

    P1507-C                                       Connected

  RSNG                                            Connected       Configured

    P1550-C                                       Connected
    P1571-C                                       Connected

Interconnect device
  IC-F4912                                        Connected       Configured

    F4912/RE0                                     Connected

Fabric manager
  FM-0                                            Connected       Configured

Fabric control
  FC-0                                            Connected       Configured

  FC-1                                            Connected       Configured

Diagnostic routing engine
  DRE-0                                           Connected       Configured
```

Verifying a Network Node Group Nonstop Software Upgrade

Purpose During the network Node group portion of a nonstop software upgrade, you should expect to see the backup network Node group Routing Engine upgrade first, followed by the Node devices within the network Node group upgrading one at a time, and ending with the upgrade of the master network Node group Routing Engine. In addition to the steps below, you can issue the **show system software upgrade status** command to view the progress of the upgrade.

NOTE: If you configure an upgrade group for Node groups containing 2 or more Node devices, all Node devices within the upgrade group reboot at the same time.

Action 1. In an SSH session to the QFabric CLI, issue the request for the network Node group nonstop software upgrade.

```
root@qfabric>  request system software nonstop-upgrade node-group NW-NG-0
jinstall-qfabric-12.2X50-D10.3.rpm
Upgrading target(s): NW-NG-0

[NW-NG-0  2012-06-01 09:45:06]: Starting with package
ftp://169.254.0.3/pub/images/12.2X50-D10.3/jinstall-qfx.tgz
[NW-NG-0  2012-06-01 09:45:06]: Retrieving package
[NW-NG-0  2012-06-01 09:46:18]: Pushing bundle to fpc0
[NW-NG-0  2012-06-01 09:46:52]: fpc0: Validate package...
[NW-NG-0  2012-06-01 09:53:26]: ------- fpc0 -------
[NW-NG-0  2012-06-01 09:54:01]: Step 1 of 20 Creating temporary file system
[NW-NG-0  2012-06-01 09:54:01]: Step 2 of 20 Determining installation source
[NW-NG-0  2012-06-01 09:54:02]: Step 3 of 20 Processing format options
[NW-NG-0  2012-06-01 09:54:02]: Step 4 of 20 Determining installation slice
[NW-NG-0  2012-06-01 09:54:02]: Step 5 of 20 Creating and labeling new slices
[NW-NG-0  2012-06-01 09:54:03]: Step 6 of 20 Create and mount new file system
[NW-NG-0  2012-06-01 09:54:10]: Step 7 of 20 Getting OS bundles
[NW-NG-0  2012-06-01 09:54:10]: Step 8 of 20 Updating recovery media
[NW-NG-0  2012-06-01 09:54:31]: Step 9 of 20 Extracting incoming image
[NW-NG-0  2012-06-01 09:55:43]: Step 10 of 20 Unpacking OS packages
[NW-NG-0  2012-06-01 09:55:46]: Step 11 of 20 Mounting jbase package
[NW-NG-0  2012-06-01 09:56:09]: Step 12 of 20 Creating base OS symbolic links
[NW-NG-0  2012-06-01 09:57:05]: Step 13 of 20 Creating fstab
[NW-NG-0  2012-06-01 09:57:05]: Step 14 of 20 Creating new system files
[NW-NG-0  2012-06-01 09:57:05]: Step 15 of 20 Adding jbundle package
[NW-NG-0  2012-06-01 09:59:30]: Step 16 of 20 Backing up system data
[NW-NG-0  2012-06-01 09:59:44]: Step 17 of 20 Setting up shared partition data
[NW-NG-0  2012-06-01 09:59:44]: Step 18 of 20 Checking package sanity in
installation
[NW-NG-0  2012-06-01 09:59:44]: Step 19 of 20 Unmounting and cleaning up
temporary file systems
[NW-NG-0  2012-06-01 09:59:47]: Step 20 of 20 Setting da0s1 as new active
partition
[NW-NG-0  2012-06-01 09:59:55]: Starting with package
ftp://169.254.0.3/pub/images/12.2X50-D10.3/jinstall-dc-re.tgz
[NW-NG-0  2012-06-01 09:59:55]: Retrieving package
[NW-NG-0  2012-06-01 10:01:04]: Pushing bundle to re1
[NW-NG-0  2012-06-01 10:01:35]: re1: Validate package...
[NW-NG-0  2012-06-01 10:02:56]: re0: Validate package...
[NW-NG-0  2012-06-01 10:04:45]: Rebooting Backup RE
[NW-NG-0  2012-06-01 10:08:31]: Initiating Chassis In-Service-Upgrade
[NW-NG-0  2012-06-01 10:08:52]: Upgrading group: 0 fpc: 0
[NW-NG-0  2012-06-01 10:18:33]: Upgrade complete for group:0
[NW-NG-0  2012-06-01 10:18:33]: Finished processing all upgrade groups, last
group :0
[NW-NG-0  2012-06-01 10:18:37]: Preparing for Switchover
[NW-NG-0  2012-06-01 10:18:55]: Switchover Completed
[Status   2012-06-01 10:18:58]: Upgrade completed with 0 errors
Success
```

2. Issue the **show system software upgrade status** command to view the status of the upgrade.

   root@qfabric> show system software upgrade status
   ```
   Wed Jan 16 22:06:02 2013 Software nonstop upgrade on:
                            NW-NG-0 in progress
   ```

3. Verify the progress of the upgrade by issuing the **show chassis nonstop-upgrade node-group**, **show fabric administration inventory**, **show fabric administration inventory infrastructure**, and **show fabric administration inventory node-groups NW-NG-0** commands. You should see the backup network Node group Routing Engine reboot first, followed by each Node device within the network Node group, and ending with the reboot of master network Node group Routing Engine. Restarting devices appear as **Disconnected** in the output of the **show fabric administration inventory** command and restarting Routing Engines do not appear in output of the **show fabric administration inventory infrastructure** command until they return to service.

Related Documentation

- *Nonstop Software Upgrade Checklist for QFabric Systems*
- *Performing a Nonstop Software Upgrade on the QFabric System*
- Understanding Nonstop Software Upgrade for QFabric Systems on page 154
- **show chassis nonstop-upgrade node-group on page 411**
- *show fabric administration inventory*
- *show fabric administration inventory director-group status*
- *show fabric administration inventory infrastructure*
- *show fabric administration inventory interconnect-devices*
- *show fabric administration inventory node-groups*

Upgrading Software by Using Automatic Software Download

The automatic software download feature uses the Dynamic Host Configuration Protocol (DHCP) message exchange process to download and install software packages. You configure the automatic software download feature on switches that act as DHCP clients. You must enable automatic software download on a switch before the software upgrade can occur.

You configure a path to a software package file on the DHCP server. The server communicates the path to the software package file through DHCP server messages.

If you enable automatic software download, the DHCP client switch compares the software package name in the DHCP server message with the name of the software package that booted the switch. If the software packages are different, the DHCP client switch downloads and installs the software package specified in the DHCP server message.

Before you upgrade software by using automatic software download, ensure that you have configured DHCP services for the switch, including configuring a path to a boot server and a boot file.

To configure a path to a boot server and a boot file:

1. Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup. This configuration is equivalent to DHCP Option 66:

   [edit system services dhcp]
   user@switch# **set boot-server (*address* | *hostname*)**

2. Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete the DHCP setup. This configuration is equivalent to DHCP Option 67:

   [edit system services dhcp]
   user@switch# **set boot-file *filename***

To enable automatic software download on a switch that acts as a DHCP client:

[edit chassis]
user@switch# **set auto-image-upgrade**

After automatic software download is enabled on your DHCP client switch and after DHCP services are enabled on your network, an automatic software download can occur at any time as part of the DHCP message exchange process.

If an automatic software download occurs, you see the following message on the switch:

Auto-image upgrade started
On successful installation system will reboot automatically

The switch reboots automatically to complete the upgrade.

Related Documentation

- Verifying That Automatic Software Download Is Working Correctly on page 179
- Understanding Software Installation on EX Series Switches on page 35
- *Configuring a DHCP Server on Switches (CLI Procedure)*
- *Configuring DHCP Services (J-Web Procedure)*
- *Understanding DHCP Services for Switches*

Verifying That Automatic Software Download Is Working Correctly

Purpose Verify that the automatic software download feature is working correctly.

Action Use the **show system services dhcp client *interface-name*** command to verify that the automatic software download feature has been used to install a software package.

```
user@switch> show system services dhcp client ge-0/0/1.0
 Logical Interface Name       ge-0/0/1.0
  Hardware address        00:0a:12:00:12:12
  Client Status           bound
  Vendor Identifier       ether
  Server Address          10.1.1.1
  Address obtained        10.1.1.89
  Lease Obtained at       2009-08-20 18:13:04 PST
  Lease Expires at        2009-08-22 18:13:04 PST

DHCP Options :
  Name: name-server, Value: [ 10.209.194.131, 2.2.2.2, 3.3.3.3 ]
  Name: server-identifier, Value: 10.1.1.1
  Name: router, Value: [ 10.1.1.80 ]
  Name: boot-image,
  Value: jinstall-ex-4200-9.6R1.5-domestic-signed.tgz
  Name: boot-image-location,
  Value: 10.1.1.25:/bootfiles/
```

Meaning The output from this command shows the name and location of the software package under DHCP options when automatic software download was last used to install a software package. The sample output in DHCP options shows that the last DHCP server message to arrive on the DHCP client had a boot server address of 192.168.1.165 and a boot file named jinstall-ex-4200-9.6R1.5-domestic-signed.tgz. If automatic software download was enabled on this client switch during the last DHCP message exchange, these values were used by the switch to upgrade the software.

Related Documentation

- Upgrading Software by Using Automatic Software Download on page 178
- *Understanding DHCP Services for Switches*

Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch

Before or after upgrading or downgrading Junos OS, you might need to verify the Junos OS version. You might also need to verify the boot loader software version if you are upgrading to or downgrading from a release that supports resilient dual-root partitions (Junos OS Release 10.4R3 and later).

This topic includes:

Verifying the Number of Partitions and File System Mountings

Purpose Between Junos OS Release 10.4R2 and Release 10.4R3, upgrades were made to further increase resiliency of root partitions, which required reformatting the disk from three partitions to four partitions. If your switch is running Release 10.4R2 or earlier, it has three partitions, and if it is running Release 10.4R3 or later, it has four partitions.

Action Verify how many partitions the disk has, as well as where each file system is mounted, by using the following command:

```
user@switch> show system storage
fpc0:
--------------------------------------------------------------------------
Filesystem  Size  Used  Avail  Capacity Mounted on
/dev/da0s1a 184M  124M    45M     73%    /
devfs       1.0K  1.0K    0B      100%  /dev
/dev/md0     37M   37M    0B      100%  /packages/mnt/jbase
/dev/md1     18M   18M    0B      100%
/packages/mnt/jcrypto-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md2    6.1M  6.1M    0B      100%
/packages/mnt/jdocs-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md3    154M  154M    0B      100%
/packages/mnt/jkernel-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md4     23M   23M    0B      100%
/packages/mnt/jpfe-ex42x-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md5     46M   46M    0B      100%
/packages/mnt/jroute-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md6     28M   28M    0B      100%
/packages/mnt/jswitch-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md7     22M   22M    0B      100%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md8     126M  10.0K 116M       0%  /tmp
/dev/da0s3e  123M   632K  112M     1%  /var
/dev/da0s3d  369M    20K  339M     0%  /var/tmp
/dev/da0s4d   62M    62K   57M     0%  /config
/dev/md9     118M   12M   96M     11%  /var/rundb
procfs       4.0K  4.0K    0B    100%  /proc
/var/jail/etc 123M  632K 112M      1%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/var/etc
/var/jail/run 123M   632K 112M    1%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/var/run
/var/jail/tmp 123M   632K 112M    1%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/var/tmp
/var/tmp      369M    20K 339M    0%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/var/tmp/uploads
devfs         1.0K   1.0K   0B  100%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/dev
```

Meaning The presence of the partition name containing **s4d** indicates that there is a fourth slice. If this were a three-slice partition scheme, in place of **s1a**, **s3e**, **s3d**, and **s4d**, you would see **s1a**, **s1f**, **s2a**, **s2f**, **s3d**, and **s3e** and you would not see **s4d**.

Verifying the Loader Software Version

Purpose For the special case of upgrading from Junos OS Release 10.4R2 or earlier to Release 10.4R3 or later, you must upgrade the loader software.

Action For EX Series switches except EX8200 switches:

```
user@switch> show chassis firmware
Part                    Type       Version
FPC 0                   uboot      U-Boot 1.1.6 (Jan  3 2011 - 16:14:58) 1.0.0

                        loader     FreeBSD/PowerPC U-Boot bootstrap loader 2.4
```

For EX8200 switches:

```
user@switch> show chassis firmware
Part                    Type       Version
FPC 0                   uboot      U-Boot 1.1.6 (Jan  3 2011 - 16:14:58) 3.5.0

                        loader     FreeBSD/PowerPC U-Boot bootstrap loader 2.4
```

Meaning For EX Series switches other than EX8200 switches, with Junos OS Release 10.4R3 or later installed:

- If there is version information following the timestamp for **U-Boot** (**1.0.0** in the preceding example), then the loader software does not require upgrading.
- If there is no version number following the timestamp for **U-boot**, then the loader software requires upgrading.

NOTE: **If the software version is Release 10.4R2 or earlier, no version number is displayed following the timestamp for U-boot, regardless of the loader software version installed. If you do not know whether you have installed the new loader software, we recommend that you upgrade the loader software when you upgrade the software version.**

For EX8200 switches, if the version number following the timestamp for **U-Boot** is earlier than **3.5.0**, you must upgrade the loader software when you upgrade the software version.

Verifying Which Root Partition Is Active

Purpose Switches running Release 10.4R3 or later have resilient dual-root partition functionality, which includes the ability to boot transparently from the inactive partition if the system fails to boot from the primary root partition.

You can verify which root partition is active using the following command:

Action

```
user@switch> show system storage partitions
fpc0:
--------------------------------------------------------------------------
Boot Media: internal (da0)
Active Partition: da0s1a
Backup Partition: da0s2a
Currently booted from: active (da0s1a)

Partitions information:
  Partition  Size   Mountpoint
  s1a        184M   /
  s2a        184M   altroot
  s3d        369M   /var/tmp
  s3e        123M   /var
  s4d        62M    /config
  s4e               unused (backup config)
```

Meaning The **Currently booted from:** field shows which root partition is active.

Verifying the Junos OS Version in Each Root Partition

Purpose Each switch contains two root partitions. We recommend that you copy the same Junos OS version in each partition when you upgrade. In Junos OS Release 10.4R2 and earlier, you might choose to have different Junos OS release versions in each partition. You might have different versions during a software upgrade and before you have finished verifying the new software installation. To enable a smooth reboot if corruption is found in the primary root file system, ensure that the identical Junos OS images are in each root partition. For Release 10.4R2 and earlier, you must manually reboot the switch from the backup root partition. However, for Release 10.4R3 and later, the switch reboots automatically from the backup root partition if it fails to reboot from the active root partition.

Action Verify whether both root partitions contain the same image by using the following command:

```
user@switch> show system snapshot media internal
Information for snapshot on       internal (/dev/da0s1a) (backup)
Creation date: Jan 11 03:02:59 2012
JUNOS version on snapshot:
  jbase  : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
Information for snapshot on       internal (/dev/da0s2a) (primary)
Creation date: Mar 6 02:24:08 2012
JUNOS version on snapshot:
  jbase  : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
```

Meaning The command shows which Junos OS version is installed on each media partition. Verify that the same version is installed on both partitions.

Related Documentation

- Troubleshooting Software Installation on page 321
- Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 324
- Understanding Resilient Dual-Root Partitions on Switches on page 93
- Resilient Dual-Root Partitions Frequently Asked Questions on page 102

Upgrading the Loader Software on the Line Cards in a Standalone EX8200 Switch or an EX8200 Virtual Chassis

You are almost never required to upgrade the loader software on the line cards in an EX8200 switch.

Upgrading the loader software version for a line card is not a requirement to complete any software upgrade. In rare cases, a line card might go offline immediately after a software upgrade because the loader software version on the line card requires an upgrade to become compatible with the upgraded Junos OS. You can upgrade the loader software on the line cards as a best practice to avoid this problem and other less severe issues.

The loader software on any line card in an EX8200 switch is updated using the same loader software package that upgrades the EX8200 Routing Engine loader software. The line card software loader contains two banks, each with a single loader software version. This procedure is used to upgrade the loader software for both banks of a line card in a standalone EX8200 switch or an EX8200 Virtual Chassis.

NOTE: If you are upgrading Junos OS, the Routing Engine loader software, and the line card loader software, we recommend that you upgrade in this order: Junos OS, line card loader software, Routing Engine loader software.

1. Determine the version of the loader software for the line cards:

```
user@switch> show chassis firmware
Part              Type       Version
FPC 6             U-Boot     U-Boot 1.1.6 (Jan 13 2009 - 06:55:22) 2.3.0
                  loader     FreeBSD/PowerPC U-Boot bootstrap loader 2.2
FPC 7             U-Boot     U-Boot 1.1.6 (Jan 13 2009 - 06:55:22) 2.3.0
                  loader     FreeBSD/PowerPC U-Boot bootstrap loader 2.2
Routing Engine 0  U-Boot     U-Boot 1.1.6 (Mar 11 2011 - 04:29:01) 3.5.0
                  loader     FreeBSD/PowerPC U-Boot bootstrap loader 2.4
Routing Engine 1  U-Boot     U-Boot 1.1.6 (Mar 11 2011 - 04:29:01) 2.3.0
                  loader     FreeBSD/PowerPC U-Boot bootstrap loader 2.4
```

NOTE: On an EX8200 Virtual Chassis, you cannot execute the **show chassis firmware** command on the master external Routing Engine. You must execute this command on each member switch:

1. From the master external Routing Engine, start a shell session on the member switch. For example:

   ```
   user@external-routing-engine> request session member 0
   ```

2. Enter the CLI and execute the **show chassis firmware** command.
3. Repeat these steps for the other member switch.

The loader software version appears after the timestamp for **U-Boot 1.1.6**. In the preceding example, the version is **2.3.0**. Ignore the U-Boot version number (**1.1.6**); it has nothing to do with the loader software version that you need to determine.

If the loader software version is earlier than **3.5.0** for any **FPC**, you should consider upgrading the loader software for that line card.

2. Download the loader software package from the Juniper Networks website and place the software package on an internal software distribution site or in a local directory on the switch. We recommend using **/var/tmp** as the local directory on the switch.

NOTE: To obtain the loader software package, see the Download Software page at http://www.juniper.net/support/downloads/junos.html. Click on the version, then the Software tab, and then the name of the software install package. In the pop-up Alert box, click the link to the PSN document.

3. Disable graceful Routing Engine switchover (GRES) and nonstop active routing (NSR), if enabled. Commit the configuration:

```
user@switch# deactivate chassis redundancy graceful-switchover
user@switch# deactivate routing-options nonstop-routing
user@switch# commit synchronize
```

4. Install the loader package:

```
user@switch> request system software add package
```

Replace ***package*** with one of the following paths:

- For a software package in the **/var/tmp** directory on the switch or external Routing Engine—**/var/tmp/*package*.tgz**
- For a software package on a remote server:
  - **ftp://*hostname/pathname/package*.tgz**
  - **http://*hostname/pathname/package*.tgz**

  where ***package*.tgz** is, for example, **jloader-ex-8200-11.3*build*-signed.tgz**.

5. Upgrade the loader software.
   - To upgrade the loader software for a line card on a standalone EX8200 switch:

     ```
     user@switch> request system firmware upgrade fpc slot slot-number
     Firmware upgrade initiated....
     Please wait for ~2mins for upgrade to complete....
     ```

   - To upgrade the loader software for a line card on an EX8200 member switch in an EX8200 Virtual Chassis:

     ```
     user@switch> request system firmware upgrade fpc slot slot-number member member-id

     Firmware upgrade initiated....
     Please wait for ~2mins for upgrade to complete....
     ```

6. Confirm the loader software upgrade:

   ```
   user@switch> show system firmware
   Part             Type           Tag Current   Available Status
                                       version   version
   FPC 6            U-Boot         0   2.3.0               UPGRADED SUCCESSFULLY
   FPC 7            U-Boot         0   2.3.0               OK
   Routing Engine 0 RE BIOS        0   3.1.1               OK
   Routing Engine 1                0   3.1.1               OK
   ```

   The status is **UPGRADED SUCCESSFULLY** if the boot loader version update process is complete.

   The status is **PROGRAMMING** if the boot loader version update process is still in progress.

   Do not proceed to the next step until the **show system firmware** output confirms that the loader software upgrade is complete.

7. Restart the line card.
   - To restart a line card on a standalone EX8200 switch:

     ```
     user@switch> request chassis fpc restart slot slot-number
     ```

   - To restart a line card on an EX8200 member switch in an EX8200 Virtual Chassis:

     ```
     user@switch> request chassis fpc restart slot slot-number member member-id
     ```

     NOTE: You can monitor the status of the line card restart by using the **show chassis fpc** command.

8. After the line card restart has completed, confirm the loader software version update:

```
user@switch> show chassis firmware
Part             Type           Tag Current   Available Status
                                    version   version
FPC 6            U-Boot         0   3.5.0               OK
FPC 7            U-Boot         0   2.3.0               OK
Routing Engine 0 RE BIOS        0   3.1.1               OK
Routing Engine 1                0   3.1.1               OK
```

The current version has updated to **3.5.0**. You have upgraded the loader software for one bank of the line card.

9. Repeat Steps 4 through 7 to upgrade the loader software on the other bank of the line card.

   NOTE: A bank switchover occurs automatically as part of the line card restart. Repeating Steps 3 through 6 updates the loader software on the other bank.

10. Repeat Steps 4 through 8 for all other line cards that require a line card loader version upgrade.

Related Documentation

- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) on page 132
- Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure) on page 140
- *Troubleshooting an EX8200 Line Card's Failure to Power On*

Understanding Junos OS Upgrades for J Series and SRX Series Devices

The J Series devices and SRX Series devices are delivered with Junos OS preinstalled on them. When you power on a device, it starts (boots) up using its primary boot device. These devices also support secondary boot devices, allowing you to back up your primary boot device and configuration.

As new features and software fixes become available, you must upgrade Junos OS to use them. Before an upgrade, we recommend that you back up your primary boot device.

Understanding Junos OS Upgrades for SRX Series Devices

On a services gateway, you can configure the primary or secondary boot device with a snapshot of the current configuration, default factory configuration, or rescue configuration. You can also replicate the configuration for use on another device.

If the SRX Series device does not have a secondary boot device configured and the primary boot device becomes corrupted, you can reload the Junos OS package onto the corrupted internal media from a USB flash drive or TFTP server.

Understanding Junos OS Upgrades for J Series Devices

On a J Series device, you can configure the primary or secondary boot device with a snapshot of the current configuration, default factory configuration, or rescue configuration. You can also replicate the configuration for use on another device, or configure a boot device to receive core dumps for troubleshooting.

If the J Series device does not have a secondary boot device configured and the primary boot device becomes corrupted, you can reload the Junos OS package onto the corrupted CompactFlash (CF) card with either a UNIX or Microsoft Windows computer.

NOTE: The terms *Junos OS (legacy services)* and *Junos OS* are used frequently in this section. Junos OS (legacy services) denotes the packet-based software for the J Series device, whereas Junos OS denotes the flow-based software for the J Series device.

Junos OS Upgrade Methods on the SRX Series Devices

SRX Series devices that ship from the factory with Junos OS Release 10.0 or later are formatted with the dual-root partitioning scheme.

Existing SRX Series devices that are running Junos OS Release 9.6 or earlier use the single-root partitioning scheme. While upgrading these devices to Junos OS Release 10.0 or later, you can choose to format the storage media with dual-root partitioning (strongly recommended) or retain the existing single-root partitioning.

Certain Junos OS upgrade methods format the internal media before installation, whereas other methods do not. To install Junos OS Release 10.0 or later with the dual-root partitioning scheme, you must use an upgrade method that formats the internal media before installation.

NOTE: If you are upgrading to Junos OS Release 10.0 without transitioning to dual-root partitioning, use the conventional CLI and J-Web user interface installation methods.

These upgrade methods format the internal media before installation:

- Installation from the boot loader using a TFTP server
- Installation from the boot loader using a USB storage device
- Installation from the CLI using the **partition** option (available in Junos OS Release 10.0)
- Installation using the J-Web user interface

These upgrade methods retain the existing partitioning scheme:

- Installation using the CLI
- Installation using the J-Web user interface

WARNING: Upgrade methods that format the internal media before installation wipe out the existing contents of the media. Only the current configuration will be preserved. Any important data should be backed up before starting the process.

NOTE: Once the media has been formatted with the dual-root partitioning scheme, you can use conventional CLI or J-Web user interface installation methods, which retain the existing partitioning and contents of the media, for subsequent upgrades.

Related Documentation

- Software Naming Convention (SRX Series and J Series Devices) on page 8
- *Preparing the USB Flash Drive and Upgrading the Boot Loader for SRX Series Devices*
- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- Installing Junos OS Upgrade Packages on J Series and SRX Devices from a Remote Server on page 193
- *Installation and Upgrade Guide*
- *Junos OS Administration Library for Routing Devices*

Preparing Your J Series and SRX Series Device for Junos OS Upgrades

Before you begin upgrading Junos OS on a J Series device and an SRX Series device, ensure the following:

- Obtain a Juniper Networks Web account and a valid support contract. You must have an account to download software upgrades. To obtain an account, complete the registration form at the Juniper Networks website: https://www.juniper.net/registration/Register.jsp.
- Back up your primary boot device onto a secondary storage device.

  Creating a backup has the following advantages:

  - The device can boot from backup and come back online in case of failure or corruption of the primary boot device in the event of power failure during an upgrade.
  - Your active configuration files and log files are retained.
  - The device can recover from a known, stable environment in case of an unsuccessful upgrade.

You can use either the J-Web user interface or the CLI to back up the primary boot device on the secondary storage device.

- Preparing Your SRX Series Device for Junos OS Upgrades on page 191
- Preparing Your J Series Device for Junos OS Upgrades on page 191
- Verifying Available Disk Space on SRX Series Devices on page 192

Preparing Your SRX Series Device for Junos OS Upgrades

You can use either the J-Web user interface or the CLI to back up the primary boot device on the secondary storage device.

Table 20 on page 191 lists the secondary storage devices available on an SRX Series devices.

Table 20: Secondary Storage Devices for SRX Series Devices

Storage Device	Available on Services Gateways	Minimum Storage Required
USB storage device	SRX100, SRX210, SRX220, and SRX240 Services Gateways	1 GB
	SRX650 Services Gateway	2 GB
External CompactFlash (CF)	SRX650 Services Gateway	2 GB

NOTE:

- During a successful upgrade, the upgrade package completely reinstalls the existing Junos OS. It retains configuration files, log files, and similar information from the previous version.
- After a successful upgrade, remember to back up the new current configuration to the secondary device.

Preparing Your J Series Device for Junos OS Upgrades

You can use either the J-Web user interface or the CLI to back up the primary boot device on the secondary storage device.

Table 21 on page 191 lists the secondary storage devices available in a J Series device for backup.

Table 21: Secondary Storage Devices for Backup

Storage Device	Available on J Series Devices	Minimum Storage Required
External CompactFlash (CF) card	J2320 and J2350	512 MB

NOTE:

- During a successful upgrade, the upgrade package completely reinstalls the existing Junos OS. It retains configuration files, log files, and similar information from the previous version.
- After a successful upgrade, back up the new current configuration to the secondary device.

NOTE: Previously, upgrading images on J Series devices with a 256 MB CF card from Junos OS Release 8.5 and earlier involved removing unwanted files in the images and removing the Swap Partition. From Junos OS Release 9.2 and later, as an alternative, Junos OS accomplishes the upgrade efficiently to take another snapshot of the CF card, install the image, and restore configurations.

Verifying Available Disk Space on SRX Series Devices

The amount of free disk space necessary to upgrade a device with a new version of the Junos OS can vary from one release to another. Check the Junos OS software version you are installing to determine the free disk space requirements.

If the amount of free disk space on a device is insufficient for installing the Junos OS, you might receive a warning similar to the following messages, that the /var filesystem is low on free disk space:

WARNING: The /var filesystem is low on free disk space.

WARNING: This package requires 1075136k free, but there is only 666502k available.

To determine the amount of free disk space on the device, issue the **show system storage detail** command. The command output displays statistics about the amount of free disk space in the device file systems.

A sample of the **show system storage detail** command output is shown below:

```
user> show system storage detail

Filesystem        1024-blocks       Used      Avail   Capacity   Mounted on
/dev/da0s2a            300196     154410     121772        56%   /
devfs                       1          1          0       100%   /dev
/dev/md0               409000     409000          0       100%   /junos
/cf                    300196     154410     121772        56%   /junos/cf
devfs                       1          1          0       100%   /junos/dev/
procfs                      4          4          0       100%   /proc
/dev/bo0s3e             25004         52      22952         0%   /config
/dev/bo0s3f            350628     178450     144128        55%   /cf/var
/dev/md1               171860      16804     141308        11%   /mfs
/cf/var/jail           350628     178450     144128        55%   /jail/var
/cf/var/log            350628     178450     144128        55%   /jail/var/log
devfs                       1          1          0       100%   /jail/dev
```

```
/dev/md2                40172          4       36956          0%  /mfs/var/run/utm
/dev/md3                1884         138        1596          8%  /jail/mfs
```

Downloading Junos OS Upgrade Packages on J Series and SRX Series Devices

To download Junos OS upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. Depending on your location, select the Canada and U.S. version (domestic) or the Worldwide version (ww):
   - https://www.juniper.net/support/downloads/junos.html
   - https://www.juniper.net/support/downloads/junos.html
2. Log in to the Juniper Networks website using the username (generally your e-mail address) and password supplied by your Juniper Networks representative.
3. Select the appropriate software image for your platform.
4. Download Junos OS to a local host or to an internal software distribution site.

Related Documentation

- Understanding Junos OS Upgrades for J Series and SRX Series Devices on page 188
- Preparing Your J Series and SRX Series Device for Junos OS Upgrades on page 190
- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- Installing Junos OS Upgrade Packages on J Series and SRX Devices from a Remote Server on page 193
- *Installation and Upgrade Guide*

Installing Junos OS Upgrade Packages on J Series and SRX Devices from a Remote Server

You can use the J-Web user interface to install Junos OS packages that are retrieved with FTP or HTTP from the specified location.

NOTE: **This procedure applies only to upgrading from one Junos OS release to another.**

Before installing the Junos OS upgrade:

- Verify the available space on the internal media. Verify the available space on the CompactFlash (CF) card for J Series devices. See "Preparing Your J Series and SRX Series Device for Junos OS Upgrades" on page 190 and the *Junos OS Release Notes*
- Download the software package. See"Downloading Junos OS Upgrade Packages on J Series and SRX Series Devices" on page 193.

To install Junos OS upgrades from a remote server:

1. In the J-Web user interface, select **Maintain>Software>Install Package**.
2. On the Install Remote page, enter the required information in the fields described in Table 8 on page 65.

Table 22: Install Package Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and Junos OS package name.	Type the full address of the Junos OS package location on the FTP or HTTP server—one of the following: *ftp://hostname/pathname/package-name* *http://hostname/pathname/package-name*
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	Specifies that the device is automatically rebooted when the upgrade is complete.	Check the box if you want the device to reboot automatically when the upgrade is complete.
Do not save backup (SRX Series devices)	Specifies that the backup copy of the current Junos OS package is not saved.	Check the box if you want to save the backup copy of the Junos OS package.
Format and re-partition the media before installation (SRX Series devices)	Specifies that the storage media is formatted and new partitions are created.	Check the box if you want to format the internal media with dual-root partitioning.

3. Click **Fetch and Install Package**. Junos OS is activated after the device reboots.

Related Documentation

- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- *Installation and Upgrade Guide*

Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices

NOTE: This topic is applicable only to SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

This feature simplifies the upgrading of Junos OS images in cases where there is no console access to an SRX Series device located at a remote site. This functionality allows you to upgrade the Junos OS image with minimum configuration effort by simply copying the image onto a USB flash drive, inserting it into the USB port of the SRX Series device, and performing a few simple steps. You can also use this feature to reformat a boot device and recover an SRX Series device after boot media corruption.

You can use any USB flash drive device formatted with FAT/FAT 32 file systems for the installation process.

NOTE: **This feature is not supported on chassis clusters.**

Before you begin:

- Copy the Junos OS upgrade image and its autoinstall.conf file to the USB device.
- Ensure that adequate space is available on the SRX Series device to install the software image.

To prepare the USB flash drive and copy the Junos OS image onto the USB flash drive:

1. Insert the USB flash drive into the USB port of a PC or laptop computer running Windows.
2. From My Computer, right-click the drive Devices with Removable Storage.
3. Format the drive with the FAT/FAT32 file system.
4. Copy the Junos OS image onto the USB device.

   For the installation process to succeed, copy only one image onto the USB device. Only images named junos-srxsme* are recognized by the system.
5. Check the drive name detected in My Computer for the USB device. Open the command prompt window and type:

   echo " " > <drive-name>:\autoinstall.conf

   For example, if the drive detected is drive F, type **echo " " > F:\autoinstall.conf** at the command prompt. This empty file indicates to the system that the automatic installation of the Junos OS image from the USB device is supported.
6. (Optional) Create a text file named junos-config.conf and copy the file to the USB device. For example, the following file supports an automatic configuration update during the installation process:

```
system {
  host-name narfi-8;
  domain-name englab.juniper.net;
  domain-search [ englab.juniper.net juniper.net jnpr.net spglab.juniper.net ];
  root-authentication {
    encrypted-password "$1$6RBM/j7k$IIGQ6hBMwGxOqCnK9dlWR0"; ##
      SECRET-DATA
  }
  }
```

```
    ...
...
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 10.207.31.254;
        }
    }
```

NOTE: The junos-config.conf file is optional, and it is not necessary for the automatic installation of the Junos OS image from the USB device. You can use the junos-config.conf file for a backup configuration for recovery or if the existing configuration is accidentally deleted.

Related Documentation

- Preparing Your J Series and SRX Series Device for Junos OS Upgrades on page 190
- Downloading Junos OS Upgrade Packages on J Series and SRX Series Devices on page 193
- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- Installing Junos OS Upgrade Packages on J Series and SRX Devices from a Remote Server on page 193
- *Installation and Upgrade Guide*

Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices

This example shows how to install Junos OS upgrades on J Series and SRX Series devices.

Requirements

Before you begin:

- Verify the available space on the internal media. See "Preparing Your J Series and SRX Series Device for Junos OS Upgrades" on page 190 and the *Junos OS Release Notes*
- Download the software package. See"Downloading Junos OS Upgrade Packages on J Series and SRX Series Devices" on page 193.
- Copy the software package to the device if you are installing the software package from a local directory on the device. We recommend that you copy it to the **/var/tmp** directory.

Overview

By default, the **request system software add** ***package-name*** command uses the validate option to validate the software package against the current configuration as a prerequisite to adding the software package. This validation ensures that the device can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

In this example, add the software package junos-srxsme-10.0R2-domestic.tgz (for SRX Series devices) or junos-jsr-8.5R1.1.domestic.tgz (for J Series devices) with the following options:

- **no-copy** option to install the software package but do not save the copies of package files. You should include this option if you do not have enough space on the internal media to perform an upgrade that keeps a copy of the package on the device.
- **no-validate** option to bypass the compatibility check with the current configuration before installation starts.
- **reboot** option to reboots the device after installation is completed.

Configuration

CLI Quick Configuration

To quickly install Junos OS upgrades on J Series and SRX Series devices, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

For SRX Series devices, from operational mode, enter:

```
user@host> request system software add /var/tmp/junos-srxsme-10.0R2-domestic.tgz
  no-copy no-validate reboot
```

For J Series devices, from operational mode, enter:

```
user@host> request system software add unlink no-copy
  /var/tmp/junos-jsr-8.5R1.1.domestic.tgz
request system reboot
```

GUI Step-by-Step Procedure

To install Junos OS upgrades on J Series and SRX Series devices:

1. In the J-Web user interface, select **Maintain>Software>Upload Package**.
2. On the Upload Package page, specify the software package to upload. Click **Browse** to navigate to the software package location and select junos-srxsme-10.0R2-domestic.tgz.
3. Select the **Reboot If Required** check box to set the device to reboot automatically when the upgrade is complete.
4. Select the **Do not save backup** check box to bypass saving the backup copy of the current Junos OS package (SRX Series).
5. Click **Upload Package**. The software is activated after the device has rebooted.

6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To install Junos OS upgrades on J Series and SRX Series devices:

From operational mode, install the new package on the device with the no-copy and no-validate options, and format and re-partition the media before installation, and reboot the device after installation is completed.

To install Junos OS upgrades on SRX Series devices:

1. From operational mode, install the new package on the device

   user@host> **request system software add /var/tmp/junos-srxsme-10.0R2-domestic.tgz no-copy no-validate**

2. Reboot the device.

   user@host> **request system reboot**

To install Junos OS upgrades on J Series devices:

1. From operational mode, install the new package on the device

   user@host> **request system software add unlink no-copy /var/tmp/junos-jsr-8.5R1.1.domestic.tgz**

2. Reboot the device.

   user@host> **request system reboot**

When the reboot is complete, the device displays the login prompt.

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the Junos OS Upgrade Installation on page 198

Verifying the Junos OS Upgrade Installation

Purpose

Verify that the Junos OS upgrade was installed.

Action

From operational mode, enter the **show system** command.

Related Documentation

- Understanding Junos OS Upgrades for J Series and SRX Series Devices on page 188
- *Preparing the USB Flash Drive and Upgrading the Boot Loader for SRX Series Devices*
- Preparing Your J Series and SRX Series Device for Junos OS Upgrades on page 190
- Downloading Junos OS Upgrade Packages on J Series and SRX Series Devices on page 193
- *Installation and Upgrade Guide*

Understanding BIOS Upgrades on SRX Series Devices

Understanding Manual BIOS Upgrade Using the Junos CLI

This feature is supported on SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 devices. For these SRX Series devices, the BIOS consists of a U-boot and the Junos loader. The SRX240 and SRX650 Service Gateways also include a U-shell binary as part of the BIOS. Additionally, on SRX100, SRX110, SRX210, SRX220 and SRX240 Service Gateways, a backup BIOS is supported which includes a backup copy of the U-boot in addition to the active copy from which the system generally boots up.

Table 23 on page 199 Lists the CLI commands used for manual BIOS upgrade.

Table 23: CLI Commands for Manual BIOS Upgrade

Active BIOS	Backup BIOS
request system firmware upgrade re bios	**request system firmware upgrade re bios backup**

BIOS upgrade procedure:

1. **Install the jloader-srxsme package.**

   1. Copy the jloader-srxsme signed package to the device.

      NOTE: **The version of the jloader-srxsme package you install must match the version of Junos OS.**

   2. Install the package using the **request system software add <path to jloader-srxsme package> no-copy no-validate** command.

      root> request system software add /var/tmp/jloader-srxsme-10.2B3-signed.tgz no-copy no-validate

      ```
      Installing package '/var/tmp/jloader-srxsme-10.2B3-signed.tgz' ...
      Verified jloader-srxsme-10.2B3.tgz signed by PackageProduction_10_2_0
      Adding jloader-srxsme...
      Available space: 427640 require: 2674
      Mounted jloader-srxsme package on /dev/md5...
      Saving state for rollback ...
      ```

      root> show version

```
Model: srx240h
JUNOS Software Release [10.2B3]
JUNOS BIOS Software Suite [10.2B3]
```

NOTE: Installing the jloader-srxsme package places the necessary images under directory/boot.

2. **Verify that the required images for upgrade are installed.**

   - Use the **show system firmware** to verify that the correct BIOS image version is available for upgrade. The available version is displayed under the **Available version** column.

     root> show system firmware

```
Part              Type           Tag  Current   Available  Status
                                        version   version
 Routing Engine 0  RE BIOS        0    1.5       1.7        OK
 Routing Engine 0  RE BIOS Backup 1    1.5       1.7        OK
 Routing Engine 0  RE FPGA        11   12.3.0               OK
```

3. **Upgrade the BIOS image.**

   Active BIOS:

   1. Initiate the upgrade using the **request system firmware upgade re bios** command.

      root> request system firmware upgrade re bios

```
 Part              Type           Tag  Current   Available  Status
                                        version   version
  Routing Engine 0  RE BIOS        0    1.5       1.7        OK
  Routing Engine 0  RE BIOS Backup 1    1.5       1.7        OK
  Perform indicated firmware upgrade ? [yes,no] (no) yes

Firmware upgrade initiated.
```

   2. Monitor the upgrade status using the **show system firmware** command.

      root> show system firmware

```
 Part              Type            Tag  Current   Available   Status
                                       version   version
Routing Engine 0  RE BIOS         0    1.5       1.7        PROGRAMMING
Routing Engine 0  RE BIOS Backup  1    1.5       1.7        OK
Routing Engine 0  RE FPGA         11   12.3.0               OK
```

      root> show system firmware

```
Part              Type           Tag    Current   Available   Status
                                        version   version
Routing Engine 0  RE BIOS         0    1.5        1.7       UPGRADED
                                                             SUCCESSFULLY

Routing Engine 0  RE BIOS Backup  1    1.5        1.7        OK
Routing Engine 0  RE FPGA         11   12.3.0                OK
```

NOTE: The device must be rebooted for the upgraded active BIOS to take effect.

Backup BIOS:

1. Initiate the upgrade using the **request system firmware upgade re bios backup** command.

   root> request system firmware upgrade re bios backup

   ```
   Part              Type           Tag  Current   Available  Status
                                          version   version
    Routing Engine 0  RE BIOS        0    1.5       1.7        OK
    Routing Engine 0  RE BIOS Backup 1    1.5       1.7        OK
    Perform indicated firmware upgrade ? [yes,no] (no) yes

   Firmware upgrade initiated.
   ```

2. Monitor the upgrade status using the **show system firmware** command.

   root> show system firmware

   ```
   Part              Type           Tag  Current   Available  Status
                                          version   version
    Routing Engine 0  RE BIOS        0    1.5       1.7        OK
    Routing Engine 0  RE BIOS Backup 1    1.5       1.7        PROGRAMMING
    Routing Engine 0  RE FPGA         11   12.3.0                OK
   ```

   root> show system firmware

   ```
   Part              Type           Tag    Current   Available   Status
                                           version   version
   Routing Engine 0  RE BIOS         0     1.5        1.7          OK
   Routing Engine 0  RE BIOS Backup  1     1.7        1.7        UPGRADED
                                                                SUCCESSFULLY
   Routing Engine 0  RE FPGA         11    12.3.0                OK
   ```

Understanding Auto BIOS Upgrade Methods on the SRX Series Devices

Junos OS Release 11.1 ships with BIOS version 1.9.

For the SRX100, SRX210, SRX240, and SRX650 devices, Table 24 on page 201 lists the minimum compatible BIOS versions.

Table 24: SRX Series Services Gateways BIOS Versions

SRX100	SRX210	SRX240	SRX650
1.6	*1.5*	*1.5*	*1.5*

If the current device has a BIOS version earlier than the minimum compatible version, then the auto BIOS upgrade feature upgrades the BIOS automatically to version 1.9.

The BIOS upgrades automatically in the following scenarios:

- During Junos OS upgrade through either the J-Web user interface or the CLI.

  In this case, only the active BIOS is upgraded. The following sample output is from upgrading the Junos OS using the CLI:

  ```
  root> request system software upgrade no-copy no-validate
  junos-srxsme-10.2B2-export.tgz
  Formatting alternate root (/dev/da0s2a)...
  ```

```
/dev/da0s2a: 298.0MB (610284 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 74.50MB, 4768 blks, 9600 inodes.
super-block backups (for fsck -b #) at:
32, 152608, 305184, 457760
Saving boot file package in /var/sw/pkg/ junos-srxsme-10.2B2-export.tgz
JUNOS requires BIOS version upgrade from 0.0 to 1.7
Upgrading to BIOS 1.7 ...
Upgrading Loader...
####################################
Verifying the loader image... OK
Upgrading U-Boot...
#############################################################
Verifying the new U-Boot image... OK
WARNING: The new boot firmware will take effect when the system is rebooted.
JUNOS 10.2B2 will become active at next reboot
Saving state for rollback ...
```

- During loader installation using TFTP or USB.

  In this case, only the active BIOS is upgraded. The following sample output is from the loader installation:

```
loader> install tftp:///junos-srxsme-10.2B2-export.tgz

Downloading /junos-srxsme-10.2B2-export.tgz from 10.207.18.111 ...
Verified SHA1 checksum of /a/cf/install/junos-boot-srxsme-10.2B2-export.tgz
Verified SHA1 checksum of /a/cf/install/junos-srxsme-10.2B2-export
JUNOS requires BIOS version upgrade from 0.0 to 1.7
Upgrading to BIOS 1.7 ...
Upgrading Loader...
####################################
Verifying the loader image... OK
Upgrading U-Boot...
#############################################################
Verifying the new U-Boot image... OK
WARNING: The new boot firmware will take effect when the system is rebooted.
```

- During system boot-up.

  In this case, both the active BIOS and the backup BIOS are upgraded. The following sample output is from system boot-up:

```
JUNOS requires backup BIOS version upgrade from 0.0 to 1.7
Upgrading to BIOS 1.7 ...
Upgrading Secondary U-Boot...
#############################################################
Verifying the new U-Boot image... OK
JUNOS requires active BIOS version upgrade from 0.0 to 1.7
Upgrading to BIOS 1.7 ...
Upgrading Loader...
####################################
Verifying the loader image... OK
Upgrading U-Boot...
#############################################################
Verifying the new U-Boot image... OK
WARNING: The new boot firmware will take effect when the system is rebooted.
BIOS upgrade completed successfully, rebooting ...
```

NOTE: The SRX650 device has only one set of BIOS. There is no backup BIOS upgrade for the SRX650 device.

Disabling Auto BIOS Upgrade on SRX Series Devices

The auto BIOS upgrade feature is enabled by default. You can disable the feature using the CLI in operational mode.

To disable the automatic upgrade of the BIOS on an SRX Series device, set the **chassis routing-engine bios** command.

```
user@host> set chassis routing-engine bios no-auto-upgrade
```

NOTE: The command disables automatic upgrade of the BIOS only during Junos OS upgrade or system boot-up. It does not disable automatic BIOS upgrade during loader installation.

Related Documentation

- Understanding Junos OS Upgrades for J Series and SRX Series Devices on page 188
- Installing Junos OS on SRX Series Devices (Using Boot Loader and USB) on page 66
- *Junos OS Administration Library for Routing Devices*
- *Installation and Upgrade Guide*

Upgrading the Boot Loader on SRX Series Devices

To upgrade the boot loader to the latest version:

1. Upgrade to Junos OS Release 10.0 or later (with or without dual-root support enabled).

   The Junos OS 10.0 image contains the latest boot loader binaries in this path: **/boot/uboot, /boot/loader**.

2. Enter the shell prompt using the **start shell** command.
3. Run the following command from the shell prompt:

   bootupgrade –u /boot/uboot –l /boot/loader

NOTE: For the new version to take effect, you should reboot the system after upgrading the boot loader.

To verify the boot loader version on the SRX Series device, enter the **show chassis routing-engine bios** command.

```
user@host>   show chassis routing-engine bios
Routing Engine BIOS Version: 1.5
```

The command output displays the boot loader version.

NOTE: You can use the following commands to upgrade U-Boot or perform cyclic redundancy check (CRC):

- **bootupgrade -s -u** – To upgrade the secondary boot loader.
- **bootupgrade -c u-boot** – To check CRC of the boot loader.
- **bootupgrade -s -c u-boot** – To check CRC for the secondary boot loader.
- **bootupgrade -c loader** – To check CRC for the loader on boot loader.

Related Documentation

- Preparing Your J Series and SRX Series Device for Junos OS Upgrades on page 190
- Downloading Junos OS Upgrade Packages on J Series and SRX Series Devices on page 193
- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- Installing Junos OS Upgrade Packages on J Series and SRX Devices from a Remote Server on page 193
- *Installation and Upgrade Guide*

Overview of CoS Upgrade Requirements (Junos OS Release 11.1 or 11.2 to a Later Release)

Before you upgrade to Junos OS Release 11.3, you must deactivate the CoS configuration if the CoS configuration includes any of the following features:

- **excess-rate** option
- **strict-high** or **high** priority queues
- Any of the Junos OS Release 11.1 or 11.2 default multidestination forwarding classes

CAUTION: **If your CoS configuration contains any of the features listed above and you attempt to upgrade from Junos OS Release 11.1 or 11.2 to a later version without first editing the configuration, the Junos OS might not restart.**

Junos OS Release 11.3 and later for QFX Series no longer supports the **excess-rate** statement, the **strict** priority option, or the default multidestination forwarding classes used in Junos OS Release 11.1 and 11.2. In addition, Junos OS Release 11.3 introduces new restrictions on how to configure and use **strict-high** priority queues.

This topic does not describe how to perform the software upgrade procedure. It describes how to deactivate your CoS configuration, edit your CoS configuration, and reactivate your CoS configuration at the appropriate times.

Use the following procedure to upgrade safely from Junos OS Release 11.1 or 11.2 to a later release:

1. Deactivate the CoS configuration *before* you upgrade the software:

   ```
   user@switch# deactivate class-of-service
   ```

2. Follow the upgrade procedure to Junos OS Release 11.3 or later software.
3. Make the following changes to the CoS configuration while the CoS configuration is still deactivated:
   - Remove the **excess-rate** statement from the CoS configuration if you have used it at the **[edit class-of-service schedulers]** or **[edit class-of-service traffic-control-profiles]** hierarchy level.
   - Remove the **strict-high** and **strict** priority queue configurations if you have used them at the **[edit class-of-service schedulers]** hierarchy level.
   - Remove the default multidestination forwarding classes (**mcast-be**, **mcast-af**, **mcast-ef**, and **mcast-nc**) if you have used them at the **[edit class-of-service schedulers]**, **[edit class-of-service rewrite-rules]**, **[edit class-of-service classifiers]**, **[edit class-of-service scheduler-maps]**, or **[edit class-of-service forwarding-class-sets]** hierarchy level. Alternatively, you can change the mapping of the multidestination traffic to use the new default multidestination forwarding class (**mcast**).
4. If desired, configure **strict-high** priority queues in accordance with the Junos OS Release 11.3 or later configuration rules, and map multidestination traffic to the default multidestination forwarding class (**mcast**).

5. Activate the CoS configuration:

   ```
   user@switch# activate class-of-service
   ```

6. Commit the CoS configuration:

   ```
   user@switch# commit
   ```

NOTE: If you configured the **transmit-rate** option for any queues under the **[edit class-of-service schedulers]** hierarchy level, if the rate is configured as an exact rate in Mbps, we recommend that you reconfigure the **transmit-rate** option as a percentage. This is because the scheduler converts exact rates to percentages, and when the exact rate is below 1 Gbps, some granularity may be lost in the conversion. You can avoid this potential issue by specifying the **transmit-rate** option as a percentage.

Related Documentation

- Upgrading Software on page 112
- *Understanding CoS Classifiers*
- *Understanding CoS Output Queue Schedulers*
- *Understanding CoS Traffic Control Profiles*
- *Overview of CoS Upgrade Requirements to Junos OS Release 12.2*
- *Overview of CoS Upgrade Requirements to Junos OS Release 12.3 (QFX3500 and QFX3600 Switches) or to Junos OS Release 13.1 (QFabric Systems)*
- *Example: Configuring Unicast Classifiers*
- *Example: Configuring Queue Schedulers*
- *Example: Configuring Traffic Control Profiles (Priority Group Scheduling)*

CHAPTER 9

Booting a Device Using a System Snapshot

Understanding System Snapshot on EX Series Switches

You can create copies of the software running a Juniper Networks EX Series Ethernet Switch using the system snapshot feature. The system snapshot feature takes a "snapshot" of the files currently used to run the switch and copies them to an alternate storage location. You can then use this snapshot to boot the switch at the next bootup or as a backup boot option.

The switch can boot from either internal flash media or external (USB) flash media. The contents of the snapshot vary depending on whether you create the snapshot on the media that the switch booted from or on the media that it did not boot from:

Snapshots are particularly useful for moving files onto USB flash drives. You cannot use the **copy** command or any other file-moving technique to move files from an internal memory source to USB memory on the switch.

- If you create the snapshot on the media that the switch did not boot from, the following partitions on the boot media are included in the snapshot: **root**, **altroot**, **var**, **var/tmp**, **config**.

  The **root** partition is the primary boot partition, and the **altroot** partition is the backup boot partition.

- If you create the snapshot on the media that the switch booted from, the root partition that the switch booted from is copied to the alternate root partition. The **var**, **var/tmp**, and **config** partitions are not copied as part of the snapshot because they already exist on the boot media.

The system snapshot feature has the following limitations:

- You cannot use snapshots to move files to any destination outside the switch other than an installed external USB flash drive or switches that are members of the same Virtual Chassis as the switch on which you created the snapshot..
- Snapshot commands, like all commands executed on a Virtual Chassis, are executed on the local member switch. If different member switches request the snapshot, the snapshot command is pushed to the Virtual Chasis member creating the snapshot and is executed on that member, and the output is then returned to the switch that initiated the process. For instance, if the command to create an external snapshot on member 3 is entered on member 1, the snapshot of internal memory on member 3 is taken on external memory on member 3. The output of the process is seen on member 1. No files move between the switches.

Related Documentation

- Understanding Software Installation on EX Series Switches on page 35
- Creating a Snapshot and Using It to Boot an EX Series Switch on page 208

Creating a Snapshot and Using It to Boot an EX Series Switch

The system snapshot feature takes a “snapshot” of the files currently used to run the switch and copies them to an alternate storage location. You can then use this snapshot to boot the switch at the next bootup or as a backup boot option.

This topic includes the following tasks:

- Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch on page 208
- Creating a Snapshot on an Internal Flash Drive and Using it to Boot the Switch on page 209
- Creating a Snapshot on the Alternate Slice of the Boot Media on page 209

Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch

You can create a snapshot on USB flash memory after a switch is booted by using files stored in internal memory.

Ensure that you have the following tools and parts available before creating a snapshot on a USB flash drive:

- A USB flash drive that meets the switch USB port specifications. See *USB Port Specifications for an EX Series Switch*.

To create a snapshot on USB flash memory and use it to boot the switch:

1. Place the snapshot into USB flash memory:

   user@switch> request system snapshot **partition media external**

2. (Optional) Perform this step if you want to boot the switch now using the snapshot stored on the USB flash drive. If you created the snapshot as a backup, do not perform this step.

   - To reboot the switch using the most recently created snapshot:

user@switch> request system reboot media external

- To reboot the switch using a snapshot in a specific partition on the USB flash drive:

  user@switch> request system reboot media external slice alternate

Creating a Snapshot on an Internal Flash Drive and Using it to Boot the Switch

You can create a snapshot in internal memory after a switch is booted by using files stored in external memory.

To create a snapshot in internal memory and use it to boot the switch:

1. Place the snapshot files in internal memory:

   user@switch> request system snapshot partition media internal

2. (Optional) Perform this step if you want to boot the switch now using the newly created snapshot. If you created the snapshot as a backup, do not perform this step.

   - To reboot the switch using the most recently created snapshot:

     user@switch> request system reboot media internal

   - To reboot the switch using a snapshot in a specific partition in internal memory:

     user@switch> request system reboot media internal slice alternate

Creating a Snapshot on the Alternate Slice of the Boot Media

The alternate slice of the boot media contains a backup software image that the switch can boot from if it is unable to boot from the primary slice. When you upgrade software, the new software image gets copied only to the primary slice of the boot media.

To create a snapshot of the currently booted software image on the backup slice of the boot media:

user@switch> request system reboot slice alternate

Related Documentation

- Verifying That a System Snapshot Was Created on an EX Series Switch on page 209
- Understanding System Snapshot on EX Series Switches on page 207

Verifying That a System Snapshot Was Created on an EX Series Switch

Purpose Verify that a system snapshot was created with the proper files on an EX Series switch.

Action View the snapshot:

```
user@switch>  show system snapshot media external
Information for snapshot on       external (/dev/da1s1a) (backup)
Creation date: Mar 19 03:37:18 2012
JUNOS version on snapshot:
  jbase  : ex-12.1I20120111_0048_user
  jcrypto-ex: 12.1I20120111_0048_user
  jdocs-ex: 12.1I20120111_0048_user
  jroute-ex: 12.1I20120111_0048_user
  jswitch-ex: 12.1I20120111_0048_user
```

```
  jweb-ex: 12.1I20120111_0048_user
Information for snapshot on       external (/dev/da1s2a) (primary)
Creation date: Mar 19 03:38:25 2012
JUNOS version on snapshot:
  jbase  : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
```

Meaning The output shows the date and time when the snapshot was created and the packages that are part of the snapshot. Check to see that the date and time match the time when you created the snapshot.

You can compare the output of this command to the output of the **show system software** command to ensure that the snapshot contains the same packages as the software currently running the switch.

Related Documentation

- Creating a Snapshot and Using It to Boot an EX Series Switch on page 208

Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive

There are two methods of getting Junos OS stored on a USB flash drive before using the software to boot the switch. You can pre-install the software onto the USB flash drive before inserting the USB flash drive into the USB port, or you can use the system snapshot feature to copy files from internal switch memory to the USB flash drive.

To move files into USB flash memory by using a system snapshot and use those files to boot the switch, see "Creating a Snapshot and Using It to Boot an EX Series Switch" on page 208. We recommend that you use this method to boot the switch from a USB flash drive if your switch is running properly.

If you need to pre-install the software onto the USB flash drive, you can use the method described in this topic. Pre-installing Junos OS onto a USB flash drive to boot the switch can be done at any time and is particularly useful when the switch boots to the loader prompt because the switch cannot locate the Junos OS in internal flash memory.

Ensure that you have the following tools and parts available to boot the switch from a USB flash drive:

- A USB flash drive that meets the EX Series switch USB port specifications. See *USB Port Specifications for an EX Series Switch*.
- A computer or other device that you can use to download the software package from the Internet and copy it to the USB flash drive.

To download a Junos OS package onto a USB flash drive before inserting the USB flash drive:

1. Download the Junos OS package that you want to place onto the EX Series switch from the Internet onto the USB flash drive by using your computer or other device. See "Downloading Software Packages from Juniper Networks" on page 42.
2. Remove the USB flash drive from the computer or other device.
3. Insert the USB flash drive into the USB port on the switch.
4. This step can be performed only when the prompt for the loader script (**loader>**) is displayed. The loader script starts when the Junos OS loads but the CLI is not working for any reason or if the switch has no software installed.

   Install the software package onto the switch:

   loader> **install** ***source***

   where ***source*** represents the name and location of the Junos OS package on the USB flash drive. The Junos OS package on a flash drive is commonly stored in the root drive as the only file—for example, **file:///jinstall-ex-4200-9.4R1.5-domestic-signed.tgz**.

Related Documentation

- Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure) on page 52
- Installing Software on EX Series Switches (J-Web Procedure) on page 64
- Understanding Software Installation on EX Series Switches on page 35
- See *EX2200 Switches Hardware Overview* for USB port location.
- See *Rear Panel of an EX3200 Switch* for USB port location.
- See *Rear Panel of an EX3300 Switch* for USB port location.
- See *Rear Panel of an EX4200 Switch* for USB port location.
- See *EX4300 Switches Hardware Overview* for USB port location.
- See *Front Panel of an EX4500 Switch* for USB port location.
- See *EX4550 Switches Hardware Overview* for USB port location.
- See *Switch Fabric and Routing Engine (SRE) Module in an EX6200 Switch* for USB port location.
- See *Switch Fabric and Routing Engine (SRE) Module in an EX8208 Switch* for USB port location.
- See *Routing Engine (RE) Module in an EX8216 Switch* for USB port location.

CHAPTER 10

Performing a Recovery Installation

Creating an Emergency Boot Device

If the device's Junos OS software is damaged in some way that prevents Junos OS software from loading completely, you can use the emergency boot device to revive the device. The emergency boot device repartitions the primary disk and reloads a fresh installation of Junos OS software.

The procedures outlined in this section discuss how to create an emergency boot device for any ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus router.

To create an emergency boot device:

1. Use FTP to copy the installation media into the router's **/var/tmp** directory.
2. Insert the PC Card into the external PC Card slot or USB storage device into the USB port.

3. In the UNIX shell, navigate to the **/var/tmp** directory:

   ```
   start shell
   cd /var/tmp
   ```

4. Log in as **su**:

   ```
   su [enter]
   password: [enter SU password]
   ```

5. Issue the following commands:

   ```
   dd if=/dev/zero of=/dev/externalDrive count=20
   dd if=installMedia of=/dev/externalDrive bs=64k
   ```

   where:

   - ***externalDrive***—Refers to the removable media name of the emergency boot device. For example, the removable media name for an emergency boot device on the M120 router is *da0* for both Routing Engines. For the names of the storage media, see "Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, PTX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers)" on page 26.
   - ***installMedia***—Refers to the installation media downloaded into the **/var/tmp** directory. For example, **install-media-9.0R2.10–domestic.tgz**.

   The following code example can be used to create an emergency boot device using a PC Card on an M20 router:

   ```
   dd if=/dev/zero of=/dev/ad3 count=20
   dd if=install-media-9.0R2.10–domestic.tgz of=/dev/ad3 bs=64k
   ```

   The following code example can be used to create an emergency boot device using a USB storage device on an M120 router or a TX Matrix Plus router:

   ```
   dd if=/dev/zero of=/dev/da0 count=20
   dd if=install-media-9.0R2.10–domestic.tgz of=/dev/da0 bs=64k
   ```

6. Log out as **su**:

   ```
   exit
   ```

Creating an Emergency Boot Device

If Junos OS on the device is damaged in some way that prevents the software from loading properly, you can use an emergency boot device to repartition the primary disk and load a fresh installation of Junos OS. Use the following procedure to create an emergency boot device.

Before you begin, you need to download the installation media image for your device and Junos OS release from http://www.juniper.net/customers/support/ .

NOTE: You can create the emergency boot device on another Juniper Networks switch or router, or any PC or laptop that supports Linux. The steps you take to create the emergency boot device vary, depending on the device.

To create an emergency boot device:

1. Use FTP to copy the installation media image into the **/var/tmp** directory on the device.
2. Insert a USB device into the USB port.
3. From the Junos OS command-line interface (CLI), start the shell:

   ```
   user@device> start shell
   %
   ```

4. Switch to the root account using the **su** command:

   ```
   % su
   Password: password
   ```

   NOTE: The password is the root password for the device. If you logged in to the device as root, you do not need to perform this step.

5. Enter the following command on the device:

   ```
   root@device% dd if=/var/tmp/filename of=/dev/da1 bs=16k
   ```

   The device writes the installation media image to the USB device:

   ```
   root@device% dd if=/var/tmp/install-media-qfx3500.junos_11.1 of=/dev/da1 bs=16k
   11006+1 records in
   11006+1 records out
   180332544 bytes transferred in 71.764266 secs (2512846 bytes/sec)
   ```

6. Enter the following command:

   ```
   root@device% dd if=/var/tmp/filename of=/dev/da0 bs=1048576
   ```

   The device writes the installation media image to the USB device:

   ```
   root@device% dd if=/var/tmp/jinstall-vjunos-usb-13.2.img of=/dev/da0 bs=1048576
   11006+1 records in
   11006+1 records out
   180332544 bytes transferred in 71.764266 secs (2512846 bytes/sec)
   ```

   NOTE: The device automatically create a recovery Junos OS image.

   The “Select a recovery image” menu appears on the console when one of these switches is booted and unable to load a version of Junos OS. You can follow the instructions in the “Select a recovery image” menu to load the Junos OS image for one of these switches.

7. Log out of the shell:

   ```
   root@device% exit
   % exit
   user@device>
   ```

Related Documentation

- *USB Port Specifications for the QFX Series*
- Performing a Recovery Installation on page 227
- Performing a QFabric System Recovery Installation on the Director Group on page 229

- *Performing a Recovery Installation Using an Emergency Boot Device*

Configuring Boot Devices for J Series and SRX Series Devices

This topic includes the following sections:

Example: Configuring Boot Devices for SRX Series Devices

This example shows how to configure a boot device.

Requirements

Before you begin, ensure that the backup device has a storage capacity of at least 1 GB. See "Preparing Your J Series and SRX Series Device for Junos OS Upgrades" on page 190.

Overview

You can configure a boot device to replace the primary boot device on your SRX Series device or to act as a backup boot device. Use either the J-Web user interface or the CLI to take a snapshot of the configuration currently running on the device, or of the original factory configuration and a rescue configuration, and save it to an alternate medium.

NOTE: **For media redundancy, we recommend that you keep a secondary storage medium attached to the SRX Series device and updated at all times.**

If the primary storage medium becomes corrupted and no backup medium is in place, you can recover the primary internal media from the TFTP installation.

You can also configure a boot device to store snapshots of software failures for use in troubleshooting.

NOTE: **You cannot copy software to the active boot device.**

NOTE: **After a boot device is created with the default factory configuration, it can operate only in an internal media slot.**

This example configures a boot device to back up the currently running and active file system partitions by rebooting from internal media and including only files shipped from the factory.

Configuration

CLI Quick Configuration

To quickly configure a boot device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

user@host> **request system snapshot partition media internal factory**

GUI Step-by-Step Procedure

To configure a boot device:

1. In the J-Web user interface, select **Maintain>Snapshot**.
2. On the Snapshot page, specify the boot device to copy the snapshot to. From the Target Media list, select the **internal** boot device.
3. Select the Factory check box to copy only default files that were loaded on the internal media when it was shipped from the factory, plus the rescue configuration if one has been set.
4. Select the Partition check box to partition the medium that you are copying the snapshot to. This process is usually necessary for boot devices that do not already have software installed on them.
5. Click **Snapshot**.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a boot device:

From operational mode, create a boot device from the internal media including only files shipped from the factory that will be used to back up the currently running and active file system partitions.

user@host> **request system snapshot partition media internal factory**

Results

From configuration mode, confirm your configuration by entering the **show system snapshot media internal** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

user@host> **show system snapshot media internal**

```
Information for snapshot on       internal (/dev/ad0s1a) (backup)
Creation date: Oct 9 13:30:06 2009
JUNOS version on snapshot:
  junos  : 10.0B3.10-domestic
```

```
Information for snapshot on       internal (/dev/ad0s2a) (primary)
Creation date: Jan 6 15:45:35 2010
JUNOS version on snapshot:
  junos  : 10.2-20091229.2-domestic
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the Snapshot Information on page 218

Verifying the Snapshot Information

Purpose Verify that the snapshot information for both root partitions on SRX Series devices were configured.

Action From operational mode, enter the **show system snapshot media** command.

The command output displays the snapshot creation time and Junos OS Release version on a media for both the primary and backup roots.

NOTE: With the dual-root partitioning scheme, performing a snapshot to a USB storage device that is less than 1 GB is not supported.

NOTE: You can use the **show system snapshot media internal** command to determine the partitioning scheme present on the internal media. Information for only one root is displayed for single-root partitioning, whereas information for both roots is displayed for dual-root partitioning.

NOTE: Any removable media that has been formatted with dual-root partitioning will not be recognized correctly by the **show system snapshot** CLI command on systems that have single-root partitioning. Intermixing dual-root and single-root formatted media on the same system is strongly discouraged.

Example: Configuring Boot Devices for J Series Devices

This example shows how to configure a boot device.

- Requirements on page 219
- Overview on page 219

Requirements

Before you begin, ensure that the backup device has a storage capacity of at least 256 MB. See *Preparing Your J Series Services Router for Junos OS Upgrades*.

Overview

You can configure a boot device to replace the primary boot device on your J Series device or to act as a backup boot device. Use either the J-Web user interface or the CLI to take a snapshot of the configuration currently running on the device, or of the original factory configuration and a rescue configuration, and save it to an alternate medium.

NOTE: **For media redundancy, we recommend that you keep a secondary storage medium attached to the J Series device and updated at all times.**

If the primary storage medium becomes corrupted and no backup medium is in place, you can recover the primary CF card from a special software image. You can also configure a boot device to store snapshots of software failures, for use in troubleshooting.

NOTE:

- **You cannot copy software to the active boot device.**
- **After a boot device is created with the default factory configuration, it can operate only in an internal CF slot.**
- **After the boot device is created as an internal CF, it can operate only in an internal CF slot.**

This example configures a boot device to copy the software snapshot to the device connected to the USB port.

Configuration

CLI Quick Configuration

To quickly configure a boot device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>
request system snapshot media usb
```

GUI Step-by-Step Procedure

To configure a boot device:

1. In the J-Web user interface, select **Maintain>Snapshot**.
2. On the Snapshot page, in the Target Media field, specify **usb** as the boot device to copy the snapshot to.

3. Click **Snapshot**.
4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a boot device:

From operational mode, create a boot device on an alternate medium to replace the primary boot device or to serve as a backup.

user@host> **request system snapshot media usb**

Results

From configuration mode, confirm your configuration by entering the **show system snapshot media usb** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For USB:

user@host> **show system snapshot media usb**

```
Information for snapshot on       usb (/dev/da1s1a) (primary)
            Creation date: Jul 24 16:16:01 2009
            JUNOS version on snapshot:
            junos  : 10.0I20090723_1017-domestic
            Information for snapshot on       usb (/dev/da1s2a) (backup)
            Creation date: Jul 24 16:17:13 2009
            JUNOS version on snapshot:
            junos  : 10.0I20090724_0719-domestic
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the Snapshot Information on page 220

Verifying the Snapshot Information

Purpose

Verify that the snapshot information was configured.

Action

From operational mode, enter the **show system snapshot media** command.

Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices

Use the **set system dump-device** command to specify the medium to use for the device to store system software failure memory snapshots. In this way, when the operating system fails, if you have specified a system dump device in the configuration, the operating system preserves a snapshot of the state of the device when it failed.

After you reboot the system, the dump device is checked for a snapshot as part of the operating system boot process. If a snapshot is found, it is written to the crash dump directory on the device (**/var/crash**). The customer support team can examine this memory snapshot to help determine the cause of the system software failure.

NOTE: **If the swap partition on the dump device medium is not large enough for a system memory snapshot, either a partial snapshot or no snapshot is written into the crash dump directory.**

From operational mode, enter the **set system dump-device** command with the following syntax:

```
user@host> set system dump-device boot-device | compact-flash |
  removable-compact-flash | usb
```

Table 25 on page 221 describes the **set system dump-device** command options.

Table 25: CLI set system dump-device Command Options

Option	Description
boot-device	Uses whatever device was booted from as the system software failure memory snapshot device.
compact-flash	Uses the internal CompactFlash (CF) card as the system software failure memory snapshot device.
removable-compact-flash	Uses the CF card on the rear of the device (J2320 and J2350 only) as the system software failure memory snapshot device.
usb	Uses the device attached to the USB port as the system software failure memory snapshot device.

Related Documentation

- Preparing Your J Series and SRX Series Device for Junos OS Upgrades on page 190
- Understanding Junos OS Upgrades for J Series and SRX Series Devices on page 188
- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- *Installation and Upgrade Guide*

Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices

This topic includes the following sections:

Overview

The autorecovery feature is supported on dual-partitioned SRX100, SRX210, SRX220, SRX240, and SRX650 Services Gateways. With this feature, information on disk partitioning, configuration, and licenses is recovered automatically in the event it becomes corrupted.

Autorecovery provides the following functions:

- Detect corruption in disk partitioning during system bootup and attempt to recover partitions automatically
- Detect corruption in the Junos OS rescue configuration during system bootup and attempt to recover the rescue configuration automatically
- Detect corruption in Junos OS licenses during system bootup and attempt to recover licenses automatically

How Autorecovery Works

The feature works in the following ways:

- The feature provides the **request system autorecovery state save** command, which backs up important data such as disk partitioning information, licenses, and Junos OS rescue configuration.
- Once the backup copies are saved, they are used to check the integrity of the working copies of the data on every bootup.
- The working copies are automatically recovered if any corruption is detected.

How to Use Autorecovery

You use autorecovery in the following ways:

- Prepare the router for deployment with the necessary licenses and configuration.
- After you finalize the state, execute the **request system autorecovery state save** command to back up the state.
- After you save the state, integrity check and recovery actions (if any) occur automatically on every bootup.
- If subsequent maintenance activities change the state of the router by adding licenses or updating the configuration, you need to execute the **request system autorecovery state save** command again to update the saved state.

- Execute the **show system autorecovery state** command any time to view the status of the saved information and the integrity check status of each saved item.
- Execute the **request system autorecovery state clear** command to delete all backed up data and disable autorecovery, if required.

Data That Is Backed Up in an Autorecovery

The following data is backed up during the autorecovery process:

- Rescue configuration (regenerated from the current configuration)
- License keys
- BSD lables (disk-partitioning information)

Data is backed up only when you execute the **request system autorecovery state save** command. Disk-partitioning information is backed up automatically from factory defaults (for new systems), on installation from the boot loader, and on snapshot creation.

Troubleshooting Alarms

Table 26 on page 223 lists types of autorecovery alarms, descriptions, and required actions.

Table 26: Autorecovery Alarms

Alarm	Alarm Type	Description	Action Required
Autorecovery information needs to be saved	Minor	This alarm indicates: • Unsaved data needs to be saved, or saved data contains problems and another save is required.	• Ensure that the system has all required licenses and configuration. • Execute the **request system autorecovery state save** command.
Autorecovery has recovered corrupted information	Minor	This alarm indicates: • Boot time integrity check failed for certain items; however, the items have been recovered successfully.	• No action is required. • Alarm will be cleared on next bootup.
Autorecovery was unable to recover data completely	Major	This alarm indicates: • Boot time integrity check failed for certain items, which could not be recovered successfully.	• The system might be experiencing a fatal malfunction.

Considerations

- Devices must have dual-root partitioning for autorecovery to work.
- The **request system configuration rescue save** command regenerates the rescue configuration from the current Junos OS configuration and then saves it. Therefore, executing the **save** command overwrites any existing rescue configuration.

- In general, the saved contents of the rescue configuration are not updated automatically. If you add licenses, you should execute the **request system autorecovery state save** command again.

NOTE: The rescue configuration is backed up. If /config is corrupted, the system boots from the rescue configuration.

Related Documentation

- Configuring Boot Devices for J Series and SRX Series Devices on page 216
- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- Example: Downgrading Junos OS on J Series and SRX Series Devices on page 275
- *Installation and Upgrade Guide*

Performing a Recovery Installation

If the device's software is corrupted or otherwise damaged, you may need to perform a recovery installation, using the emergency boot device to restore the default factory installation. Once you have recovered the software you will need to restore the router or switch's configuration. You can either create a new configuration as you did when the device was shipped from the factory, or if you saved the device's previous configuration, you can simply restore that file to the system.

Depending on the situation, you should try to perform the following steps before you perform the recovery installation:

1. Ensure you have an emergency recovery disk to use during the installation. When the router or switch is first shipped, an emergency recovery disk is provided with it. For instructions on creating an emergency boot device, see "Creating an Emergency Boot Device" on page 213
2. Copy the existing configuration in the file **/config/juniper.conf.gz** from the device to a remote system. For extra safety, you can also copy the backup configurations (the files named **/config/juniper.conf.*n***, where *n* is a number from 0 through 9).

   WARNING: **The recovery installation process completely overwrites the entire contents of the fixed storage media.**

3. Copy any other stored files to a remote system as desired.

To reinstall Junos OS:

1. Insert the removable media emergency boot devce into the device.

   NOTE: **You can store a configuration on installation media such as a PC Card or USB stick.**

2. Reboot the device.

   If the CLI is still active, issue the **request system reboot** command from command mode to reboot the device.

   If the CLI is not working, manually power off the device using the main power switch, wait 10 seconds, and then power the device back on.

3. When the software prompts you with the following question, type **y**:

   ```
   WARNING: The installation will erase the contents of your disk. Do you wish
   to continue (y/n)? y
   ```

   The device copies the software from the removable media emergency boot device onto your system, occasionally displaying status messages. Copying the software can take up to 45 minutes depending on the device. When the process is complete, the router boots into Amnesiac state and the login prompt is displayed.

4. Remove the removable media emergency boot device.
5. Login as root on the device's console port and issue the **request system reboot** command from command mode to reboot the device.

   The device reboots from the boot device on which the software was just installed. When the reboot is complete, the device displays the login prompt.
6. Create a new configuration as you did when the device was shipped from the factory, or restore a previously saved configuration file to the system. For more information, see "Creating a New Configuration on a Single Routing Engine" on page 235, "Creating a New Configuration with Redundant Routing Engines" on page 240, and "Restoring a Saved Configuration" on page 246.

Performing a Recovery Installation

If Junos OS on your device is damaged in some way that prevents the software from loading correctly, you may need to perform a recovery installation using an emergency boot device (for example, a USB flash drive) to restore the default factory installation. Once you have recovered the software, you need to restore the device configuration. You can either create a new configuration as you did when the device was shipped from the factory, or if you saved the previous configuration, you can simply restore that file to the device.

You can also use a system snapshot as a bootup option when your Junos OS or configuration is damaged. The system snapshot feature takes a "snapshot" of the files currently used to run the device—the complete contents of the **/config** directories, which include the running Juniper Networks Junos OS, the active configuration, and the rescue configuration, as well as the host OS—and copies all of these files into an external USB flash drive. See *Understanding System Snapshot*.

If at all possible, you should try to perform the following steps before you perform the recovery installation:

1. Ensure that you have an emergency boot device to use during the installation. See "Creating an Emergency Boot Device" on page 214 for information on how to create an emergency boot device.
2. Copy the existing configuration in the file **/config/juniper.conf.gz** from the device to a remote system, such as a server, or to an emergency boot device. For extra safety, you can also copy the backup configurations (the files named **/config/juniper.conf.*n***, where *n* is a number from 0 through 9) to a remote system or to an emergency boot device.

   WARNING: **The recovery installation process completely overwrites the entire contents of the internal flash storage.**

3. Copy any other stored files to a remote system as desired.

To reinstall Junos OS:

1. Insert the emergency boot device into the QFX Series device.
2. Reboot the QFX Series device.

   NOTE: **Do not power off the device if it is already on.**

   ```
   [edit system]
   user@device> request system reboot
   ```

   If you do not have access to the CLI, power cycle the QFX Series device.

The emergency boot device (external USB install media) is detected. At this time, you can load the Junos OS from the emergency boot device onto the internal flash storage.

3. The software prompts you with the following options:

```
External USB install media detected.
You can load Junos from this media onto an internal drive.
Press 'y' to proceed, 'f' to format and install, or 'n' to abort.
Do you wish to continue ([y]/f/n)? f
```

4. Type **f** to format the internal flash storage and install the Junos OS on the emergency boot device onto the internal flash storage.

   If you do no want to format the internal flash storage, type **y**.

   The following messages are displayed:

```
Installing packages from external USB drive da1
Packages will be installed to da0, media size: 8G

Processing format options
Fri September  4 01:18:44 UTC 2012

-- IMPORTANT INFORMATION --
Installer has detected settings to format system boot media.
This operation will erase all data from your system.

Formatting installation disk .. this will take a while, please wait
Disabling platform watchdog - threshold 12 mins

Determining installation slice
Fri September  4 01:27:07 UTC 2012
```

5. The device copies the software from the emergency boot device, occasionally displaying status messages. Copying the software can take up to 12 minutes.

   When the device is finished copying the software, you are presented with the following prompt:

```
*** Fri September  4 01:19:00 UTC 2012***
Installation successful..
Please select one of the following options:
Reboot to installed Junos after removing install media (default) ... 1
Reboot to installed Junos by disabling install media ............... 2
Exit to installer debug shell ...................................... 3
Install Junos to alternate slice ................................... 4
Your choice: 4
NOTE: System installer will now install Junos to alternate slice
Do not power off or remove the external installer media or
interrupt the installation mechanism.
```

6. Select **4** to install Junos OS to the alternate slice of the partition, and then press Enter.

7. Remove the emergency boot device when prompted and then press Enter. The device then reboots from the internal flash storage on which the software was just installed. When the reboot is complete, the device displays the login prompt.

8. Create a new configuration as you did when the device was shipped from the factory, or restore the previously saved configuration file to the device.

Related Documentation

- Creating an Emergency Boot Device on page 214

Performing a QFabric System Recovery Installation on the Director Group

If the software on your QFabric system is damaged in some way that prevents the software from loading correctly, or you need to upgrade the software on your QFabric system, you may need to perform a recovery installation on the Director group.

If possible, perform the following steps before you perform the recovery installation:

1. Ensure that you have an emergency boot device (for example, an external USB flash drive) for each of your Director devices to use during the recovery installation.

   You can either use the external USB flash drive containing the software supplied by Juniper Networks, or you can use an external USB flash drive supplied by Juniper Networks on which you install the QFabric system install media.

2. Because the recovery installation process completely overwrites the entire contents of the Director device, make sure you back up any configuration files and initial setup information on a different external USB flash drive before you begin a recovery installation. You will need to restore this information as part of recovery process.

   Use the **request system software configuration-backup** command to back up your configuration files and initial setup information:

   `user@switch>` **request system software configuration-backup** ***path***

   NOTE: To recover the Director group, you must upgrade both Director devices in parallel. If you are recovering only one Director device in a Director group, and the software version will remain the same between the two Director devices, make sure that the other Director device is powered on and operational. If the software version of the Director device you are recovering will be different, make sure that the other Director device is powered off and is not operational.

- (Optional) Creating an Emergency Boot Device Using a Juniper Networks External Blank USB Flash Drive on page 230
- Performing a Recovery Installation Using a Juniper Networks External USB Flash Drive with Preloaded Software on page 231

(Optional) Creating an Emergency Boot Device Using a Juniper Networks External Blank USB Flash Drive

If you do not have an external USB flash drive preloaded with the software from Juniper Networks to use as an emergency boot device, you can create your own, using a blank external USB flash drive provided by Juniper Networks. Download the install media from the Juniper Networks Support website onto your UNIX workstation, uncompress and untar the software, and then burn the software image onto your Juniper Networks external USB (4-gigabyte) flash drive. Make sure you create two emergency boot devices, one for each Director device, so you can perform a recovery installation in parallel.

1. Using a Web browser, navigate to the http://www.juniper.net/support .
2. Click **Download Software**.
3. In the *Switching*box, click *Junos OS Platforms*.
4. In the *QFX Series* section, click the name of the platform for which you want to download software.
5. Click the *Software* tab and select the release number from the *Release* drop-down list.
6. Select the complete install media you want to download in the *QFabric System Install Media* section.

   A login screen appears.
7. Enter your name and password and press **Enter**.
8. Read the End User License Agreement, click the **I agree** radio button, and then click **Proceed**.
9. Log in and save the install media file to your UNIX workstation.
10. Use FTP to access the UNIX workstation where the install media resides.

    ftp ftp*://hostname/pathname install-media-qfabric-<version>*.img.tgz
11. When prompted, enter your username and password.
12. Make sure you are in binary mode by entering **binary** at the prompt.

    binary
13. Use the **get** command to transfer the installation package from the FTP host to your UNIX workstation.

    get *install-media-qfabric-<version>*.img.tgz
14. Close the FTP session:

    bye
15. Untar the *install-media-qfabric-<version>* .img.tgz file on your UNIX workstation.

    ```
    tar -xvzf install-media-qfabric-11.3X30.6.img.tgz
    ```
16. Insert a blank external USB (4-gigabyte) flash drive supplied by Juniper Networks into your UNIX workstation.
17. Burn the software image you just downloaded to your UNIX workstation onto your external USB flash drive using the **dd** command:

```
dd if=install-media-qfabric-11.3X30.6.img of=/dev/sdb bs=16k
250880+0 records in
250880+0 records out
4110417920 bytes (4.1 GB) copied, 5.10768 seconds, 805 MB/s
```

18. Perform the steps in "Performing a Recovery Installation Using a Juniper Networks External USB Flash Drive with Preloaded Software" on page 231 to continue with the recovery installation.

Performing a Recovery Installation Using a Juniper Networks External USB Flash Drive with Preloaded Software

This procedure describes how to perform a recovery installation using an external USB flash drive that contains Junos OS software.

NOTE: Since the recovery installation process completely overwrites the entire contents of the Director device, you will need to restore the required configuration files and initial setup information. The following procedure assumes you previously saved these backup files with the **request system software configuration-backup** command. Ensure that you have these backup files available on an external USB flash drive before you perform the following steps.

1. Insert the external USB flash drive into the Director device.
2. Perform one of the following tasks:
   - If you have access to the default partition, reboot the Director device by issuing the **request system reboot director-group** command.
   - If you do not have access to the default partition, power cycle the Director device.

   The following menu appears on the Director device console when the Director device boots up:

   ```
   Juniper Networks QFabric Director Install/Recovery Media
   -  To boot from the local disk, wait 10 seconds or press the Enter key.
   -  To reinstall the QFabric software on this Director device, type: install
   ```

3. Type **install** and then press **Enter** to install the software on the Director device.

   Once the installation process is complete, the Director device reboots, and the following menu appears on the Director device console:

   ```
   Juniper Networks QFabric Director Install/Recovery Media
   -  To boot from the local disk, wait 10 seconds or press the Enter key.
   -  To reinstall the QFabric software on this Director device, type: install
   ```

4. Press **Enter**.

   The Director device reboots from the local disk on which the software was just installed.

5. Log in as root on the Director device.

   The following menu appears on the Director device console:

```
Before you can access the QFabric system, you must complete the initial setup
 of the Director group by using the steps that follow.
If the initial setup procedure does not complete successfully, log out of the
 Director device and then log back in to restart
 this setup menu.

Continue?[y/n]
```

6. Enter **n** to bypass the initial setup script and enter the Director device root directory, where you can mount the external USB flash drive containing the configuration files and initial setup information.

7. Issue the **ls /mnt** command to list the *mount* directory.

   ```
   root@dg0 ~]# ls /mnt
   ```

8. Issue the **mkdir** command to create a directory within the mount directory.

   ```
   root@dg0 ~]# mkdir /mnt/myusb
   ```

9. Issue the **mount /dev/sdb2 /mnt/myusb/** command to mount the external USB flash drive to the local drive of the Director device.

   ```
   root@dg0 ~]# mount /dev/sdb2 /mnt/myusb/
   ```

10. Issue the **ls -la /mnt/myusb/** command to verify the contents of your mounted external USB flashdrive.

    ```
    root@dg0 ~]# ls -la /mnt/myusb/
    total 1770884
    drwxr-xr-x 2 root root       4096 Sep  7 05:16 .
    drwxr-xr-x 3 root root       4096 Sep  7 10:15 ..
    -rw-r--r-- 1 root root       4249 Sep  7 03:52 mybackup-20110907
    ```

11. Exit the Director device and log back in as root on the Director device.

    The following menu appears:

    ```
    Before you can access the QFabric system, you must complete the initial setup
     of the Director group by using the steps that follow.
    If the initial setup procedure does not complete successfully, log out of the
     Director device and then log back in to restart
     this setup menu.

    Continue?[y/n] y
    Initial Configuration

    You may enter the configuration manually or restore from a backup.

    Specify a backup file? [y/n] : y
    Please specify the full path of the configuration backup file. :
    /mnt/myusb/mybackup-20110907
    ```

12. Enter **y** to continue.

13. Enter **y** and specify the path to the backup configuration file located on the external USB flash drive.

    ```
    /mnt/myusb/mybackup-20110907
    ```

    The following messages appear:

    ```
    Saving temporary configuration...
    Configuring peer...
    connect error for 1.1.1.2:9001
    Configuring local interfaces...
    ```



```
Configuring interface eth0 with [10.49.213.163/24:10.49.213.254]
Configured interface eth0 with [10.49.213.163/24:10.49.213.254]
Configuring QFabric software with initial pool of 4000 MAC addresses
[00:10:00:00:00:00 - 00:10:00:00:0f:3b]
Configuring QFabric address [10.49.213.50]
Reconfiguring QFabric software static configuration
Applying the new Director Device password
Applying the QFabric component password
First install initial configuration, generating and sharing SSH keys.
First install initial configuration, generating SSH keys.
connect error for 1.1.1.2:9001
Shared SSH keys.
Configuration complete. Director Group services will auto start within 30
seconds.
```

The Director device reboots from the local disk on which the software was just installed. Exit the Director device session and log in to the QFabric default partition CLI.

14. Issue the **request system software configuration-restore** command and specify the path to the backup configuration file located on the external USB flash drive to load the previously saved QFabric system configuration.

15. From the default partition, issue the **request system reboot node-group all** command to reboot all of the Node groups in the QFabric system to ensure that all Node devices are running the same version of software as the Director-group.

    ```
    user@switch> request system reboot node-group all
    ```

16. From the default partition, issue the **request system reboot fabric** command to reboot the Interconnect devices and the other components in the fabric in the QFabric system to ensure that Interconnect devices are running the same version of software as the Director group.

    ```
    user@switch> request system reboot fabric
    ```

17. Log in to the default partition and issue the **show version component all** command to verify that all components are running the same version of software.

    ```
    user@switch> show version component all
    dg1:
    -
    Hostname: qfabric
    Model: qfx3100
    JUNOS Base Version [11.3X30.6]

    dg0:
    -
    Hostname: qfabric
    Model: qfx3100
    JUNOS Base Version [11.3X30.6]

    NW-NG-0:
    -
    Hostname: qfabric
    Model: qfx-jvre
    JUNOS Base OS boot [11.3X30.6]
    JUNOS Base OS Software Suite [11.3X30.6]
    JUNOS Kernel Software Suite [11.3X30.6]
    JUNOS Crypto Software Suite [11.3X30.6]
    JUNOS Online Documentation [11.3X30.6]
    JUNOS Enterprise Software Suite [11.3X30.6]
    JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
    ```

```
JUNOS Routing Software Suite [11.3X30.6]

FC-0:
-
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

FC-1:
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

DRE-0:
-
Hostname: dre-0
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

FM-0:
-
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

nodedevice1:
-
Hostname: qfabric
Model: QFX3500
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
```



```
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]

interconnectdevice1:
-
Hostname: qfabric
Model: QFX3108
JUNOS Base OS boot [11.3X30.6]
JUNOS Base OS Software Suite [11.3X30.6]
JUNOS Kernel Software Suite [11.3X30.6]
JUNOS Crypto Software Suite [11.3X30.6]
JUNOS Online Documentation [11.3X30.6]
JUNOS Enterprise Software Suite [11.3X30.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3X30.6]
JUNOS Routing Software Suite [11.3X30.6]
warning:  from interconnectdevice0: Disconnected
```

Related Documentation

- *Performing the QFabric System Initial Setup on a QFX3100 Director Group*
- Upgrading Software on a QFabric System on page 150
- **request system software configuration-backup on page 383**
- **request system software configuration-restore on page 384**

Creating a New Configuration on a Single Routing Engine

To create a new base configuration on a single Routing Engine:

- Log In to the Router Console on page 235
- Configure Administration User Accounts on page 236
- Add the Management Console to the Network on page 236
- Commit Changes on page 238

Log In to the Router Console

To log in to the device's console interface and open the CLI in configuration mode:

1. Verify the device is powered on.
2. Log in through the console port as root.

   Amnesiac <ttyd0>

   login: **root**

   NOTE: From the factory, the root administration user account is not associated with a password. However, you must add a password to the root administration account before you can successfully commit a configuration.

3. Start the CLI, which initially opens in operational mode. Note the command prompt ends with > in the CLI operational mode.

   root@% **cli**
   root>

4. Enter the CLI configuration mode. Note the command prompt ends with **#** in the CLI configuration mode.

   root> **configure**
   [edit]
   root#

Configure Administration User Accounts

Set the root administration user account password. You also need to set up one or more administration user accounts. These administration user accounts are used to log in to the device through the management console. To configure administration user accounts:

1. Add a password to the root (superuser) administration user account.

   [edit]
   root# **set system root-authentication plain-text-password**
   New password: *password*
   Retype new password: *password*

2. Create a management console user account.

   [edit]
   root# **set system login user** *user-name* **authentication plain-text-password**
   New Password: *password*
   Retype new password: *password*

3. Set the user account class to **super-user**.

   [edit]
   root# **set system login user** *user-name* **class super-user**

Add the Management Console to the Network

To add the management console to the network:

1. Specify the device hostname.

   NOTE: The hostname specified in the device configuration is not used by the DNS server to resolve to the correct IP address. This hostname is used to display the name of the Routing Engine in the CLI. For example, this hostname appears on the command line prompt when the user is logged in to the CLI:

   user-name@host-name>

   [edit]
   root# **set system host-name** *host-name*

2. Configure the IP address of the DNS server.

```
[edit]
root# set system name-server address
```

3. Configure the router or switch domain name.

```
[edit]
root# set system domain-name domain-name
```

4. Configure the IP address and prefix length for the router or switch Ethernet interface.

   - For all devices *except* the TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers:

     ```
     [edit]
     root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
     ```

   - For TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix only, and PTX Series Packet Transport Routers:

     ```
     [edit]
     root@# set interfaces em0 unit 0 family inet address address/prefix-length
     ```

     To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

   - For a T1600 standalone router (not connected to a TX Matrix Plus router and not in a routing matrix):

     ```
     [edit]
     root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
     ```

5. Configure the IP address of a backup router. The backup router is used while the local router is booting and if the routing process fails to start. Once the routing process starts, the backup router address is removed from the local routing and forwarding tables. For more information about the backup router, see the *Getting Started Guide for Routing Devices*.

```
[edit]
root# set system backup-router address
```

6. (Optional) Configure the static routes to remote subnets with access to the management port. Access to the management port is limited to the local subnet. To access the management port from a remote subnet, you need to add a static route to that subnet within the routing table.

```
[edit]
root# set routing-options static route remote-subnet next-hop destination-IP retain
 no-readvertise
```

7. Configure telnet service at the **[edit system services]** hierarchy level.

```
[edit]
root# set system services telnet
```

Commit Changes

Now that you have completed your changes to the configuration file, commit the configuration changes.

1. Before committing the configuration, you can review your changes to the configuration with the **show** command.

```
root# show
## Last changed: 2008-08-27 22:30:42 UTC
version 9.3B1.5;
system {
  host-name tp8;
  domain-name subnet.example.net;
  backup-router 192.168.71.254;
  root-authentication {
    encrypted-password "SABC123"; ## SECRET-DATA
  }
  name-server {
    192.168.5.68;
    172.17.28.101;
  }
  login {
    user PE1 {
      class super-user;
      authentication {
        encrypted-password ""SABC123""; ## SECRET-DATA
      }
    }
  }
  services {
    telnet;
  }
  syslog {
    user * {
      any emergency;
    }
    file messages {
      any notice;
      authorization info;
    }
    file interactive-commands {
      interactive-commands any;
    }
  }
}
interfaces {
  fxp0 {
    unit 0 {
      family inet {
        address 192.168.69.205/21;
      }
    }
  }
}
```

```
routing-options {
  static {
    route 172.16.0.0/12 {
      next-hop 192.168.71.254;
      retain;
      no-readvertise;
    }
    route 192.168.0.0/16 {
      next-hop 192.168.71.254;
      retain;
      no-readvertise;
    }
  }
}
```

On a TX Matrix Plus router and PTX Series Packet Transport Routers, the management Ethernet interface is **em0** and not **fxp0**. Therefore, when you issue the **show** command in the configuration mode, the configuration statements would be:

```
[edit]
root@ show
system {
  host-name hostname;
  domain-name domain.name;
  backup-router address ;
  root-authentication {
    (encrypted-password "password" | public-key);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
  }
  name-server {
    address;
  }
  interfaces {
    em0 {
      unit 0 {
        family inet {
          address address ;
        }
      }
    }
  }
}
```

2. Commit the configuration.

```
[edit]
root# commit
commit complete
```

NOTE: If you receive an error message after you issue the **commit** statement, you can review the configuration using the **show** command to find the errors in your configuration. You can delete incorrect entries using the **delete** command. For example, to delete a hostname from the configuration, issue the following statement:

```
[edit]
root# delete system host-name host-name
```

3. Exit configuration mode.

```
[edit]
root# exit
Exiting configuration mode

root>
```

Creating a New Configuration with Redundant Routing Engines

To create a new base configuration on a router with redundant Routing Engines:

- Configure Administration User Accounts on page 240
- Set Up Routing Engine Configuration Groups on page 241
- Complete the Management Console Configuration on page 242
- Commit and Synchronize Changes on page 243

Configure Administration User Accounts

Set the root administration user account password. You also need to set up one or more administration user accounts. These administration user accounts are used to log in to the device through the management console. To configure administration user accounts:

1. Add a password to the root (superuser) administration user account.

```
[edit]
root# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

2. Create a management console user account.

```
[edit]
root# set system login user user-name authentication plain-text-password
New Password: password
Retype new password: password
```

3. Set the user account class to **super-user**.

```
[edit]
root# set system login user user-name class super-user
```

Set Up Routing Engine Configuration Groups

In a router with two Routing Engines, one configuration should be shared between both Routing Engines. This ensures that both Routing Engine configurations are identical. Within this configuration, create two Routing Engine groups, one for each Routing Engine. Within these groups, you specify the Routing Engine–specific parameters.

For more information about creating configuration groups, see *CLI User Guide*.

For more information about the initial configuration for redundant Routing Engine systems and the re0 group, see *Junos OS High Availability Library for Routing Devices*.

1. Create the configuration group **re0**. The **re0** group is a special group designator that is only used by **RE0** in a redundant routing platform.

   [edit]
   root# **set groups re0**

2. Navigate to the **groups re0** level of the configuration hierarchy.

   [edit]
   root# **edit groups re0**

3. Specify the router hostname.

   [edit groups re0]
   root# **set system host-name** ***host-name***

   NOTE: The hostname specified in the router configuration is not used by the DNS server to resolve to the correct IP address. This hostname is used to display the name of the Routing Engine in the CLI. For example, the hostname appears at the command-line prompt when the user is logged in to the CLI:

   user-name@host-name>

4. Configure the IP address and prefix length for the router Ethernet interface.

   - For all devices *except* the TX Matrix Plus router, T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers:

     [edit]
     root@# **set interfaces fxp0 unit 0 family inet address** ***address/prefix-length***

   - For TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix only, and PTX Series Packet Transport Routers:

     [edit]
     root@# **set interfaces em0 unit 0 family inet address** ***address/prefix-length***

     To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

   - For a T1600 standalone router (not connected to a TX Matrix Plus router and not in a routing matrix):

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

5. Return to the top level of the hierarchy.

```
[edit groups re0]
root# top
```

6. Create the configuration group **re1**.

```
[edit]
root# set groups re1
```

7. Navigate to the **groups re1** level of the configuration hierarchy.

```
[edit]
root# edit groups re1
```

8. Specify the router hostname.

```
[edit groups re1]
root# set system host-name host-name
```

9. Configure the IP address and prefix length for the router Ethernet interface.

   - For all devices *except* the TX Matrix Plus router, T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers:

     ```
     [edit]
     root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
     ```

   - For TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix only:

     ```
     [edit]
     root@# set interfaces em0 unit 0 family inet address address/prefix-length
     ```

     To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

   - For a T1600 standalone router (not connected to a TX Matrix Plus router, and not in a routing matrix):

     ```
     [edit]
     root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
     ```

10. Return to the top level of the hierarchy.

```
[edit groups re0]
root# top
```

11. Specify the group application order.

```
[edit]
root# set apply-groups [ re0 re1 ]
```

Complete the Management Console Configuration

To configure the global management console parameters.

1. Configure the IP address of the DNS server.

```
[edit]
```

```
root# set system name-server address
```

2. Configure the router domain name.

```
[edit]
root# set system domain-name domain-name
```

3. Configure the IP address of a backup router. The backup router is used while the local router is booting and if the routing process fails to start. Once the routing process starts, the backup router address is removed from the local routing and forwarding tables. For more information about the backup router, see the *Getting Started Guide for Routing Devices*.

```
[edit]
root# set system backup-router address
```

4. (Optional) Configure the static routes to remote subnets with access to the management port. Access to the management port is limited to the local subnet. To access the management port from a remote subnet, you need to add a static route to that subnet within the routing table.

```
[edit]
root# set routing-options static route remote-subnet next-hop destination-IP retain
 no-readvertise
```

5. Configure telnet service at the **[edit system services]** hierarchy level.

```
[edit]
root# set system services telnet
```

Commit and Synchronize Changes

Commit the configuration changes. When you issue the **synchronize** command, the configuration is shared between both Routing Engines and committed on both Routing Engines simultaneously.

1. Before committing the configuration, you can review the configuration entries using the **show** command.

```
root# show
## Last changed: 2008-10-17 18:32:25 UTC
version 9.1R1.8;
groups {
  re0 {
    system {
      host-name spice-re0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 192.168.69.155/21;
          }
        }
      }
    }
  }
```

```
    re1 {
      system {
        host-name spice-re1;
      }
      interfaces {
        fxp0 {
          unit 0 {
            family inet {
              address 192.168.70.72/21;
            }
          }
        }
      }
    }
    global;
  }
  apply-groups [ re0 re1 ];
  system {
    domain-name devicex.example.com;
    backup-router 192.168.71.254;
    root-authentication {
      encrypted-password "$ABC123x"; ## SECRET-DATA
    }
    name-server {
      192.168.1.1;
    }
    login {
      user user {
        uid 2001;
        class super-user;
        authentication {
          encrypted-password "$ABC123x"; ## SECRET-DATA
        }
      }
    }
    services {
      telnet;
    }
    syslog {
      user * {
        any emergency;
      }
      file messages {
        any notice;
        authorization info;
      }
      file interactive-commands {
        interactive-commands any;
      }
    }
  }
  routing-options {
    static {
      /* corporate office */
      route 172.16.0.0/12 {
        next-hop 192.168.71.254;
```

```
            retain;
            no-readvertise;
        }
    }
}
```

2. Commit and synchronize the configuration. The **commit synchronize** command commits this new configuration on both Routing Engines simultaneously.

   ```
   [edit]
   root# commit synchronize
   re0:
   configuration check succeeds
   re1:
   commit complete
   re0:
   commit complete
   ```

   If you receive an error message after you issue the **commit** statement, you can review the configuration using the **show** command to find the errors in your configuration. You can delete incorrect entries using the **delete** command. For example, to delete a hostname from the configuration, issue the following command:

   ```
   [edit]
   root# delete system host-name host-name
   ```

3. Exit configuration mode.

   ```
   [edit]
   root# exit
   Exiting configuration mode

   root>
   ```

Saving a Rescue Configuration File

A rescue configuration file is helpful in the event that your device's configuration file has been misconfigured. You can restore the device to this rescue configuration to bring the device back online. If you save this file off the device, the rescue configuration can also be used to restore your device in the event of a software failure.

To save a current device configuration as a rescue configuration file:

1. Edit the configuration file on the device to reflect the base configuration you wish to use.

   For more information about editing the configuration, see *Overview for Routing Devices*.

2. In the CLI operational mode, save this edited base configuration as the rescue configuration file:

   ```
   user@host> request system configuration rescue save
   ```

   The rescue configuration file is automatically saved under **/config** directory.

3. Copy the rescue configuration to a remote server:

```
user@host1> cd/config/
user@host1> ls -ltr rescue.conf.gz

user@host1 ftp host2
Name: username
Password: password
User user logged in.
ftp> cd /var/tmp
ftp> lcd /config
ftp> bi
ftp> put rescue.conf.gz
local:  rescue.conf.gz remote: rescue.conf.gz

Transfer complete.
ftp> bye
Goodbye.
```

To roll back to the rescue configuration, use the **rollback rescue** command.

```
user@host# rollback rescue

load complete
```

NOTE: After rolling back to the rescue configuration, you must commit the configuration to activate it:

```
user@host#commit
```

Restoring a Saved Configuration

To restore a saved configuration, perform the following tasks:

1. Copy Saved Files to the Router on page 246
2. Load and Commit the Configuration File on page 247

Copy Saved Files to the Router

To copy the saved configuration to the router:

1. Log in to the console as **root**. There is no password.

   ```
   Escape character is '^]'.
   [Enter]
   router (ttyd0)

   login: root
   Password: [Enter]
   ```

   Initially, access to the router is limited to the console port after a recovery installation. Access through the management ports and interfaces is set in the configuration. For information about accessing the router through the console port, see the administration guide for your particular router.

2. Start the CLI:


```
# cli
```

3. Copy the configuration file on the remote server to the router's **/var/tmp** directory:

```
root@host> ftp remote-server
user: username
password: password
ftp> bin
Type set to I.
ftp> get /path/file
ftp> bye
Goodbye.
```

Load and Commit the Configuration File

Once the saved configuration file is copied to the router, you load and commit the file:

1. Start the CLI configuration mode.

```
user@routername> configure
Entering configuration mode

[edit]
user@host#
```

2. Load the file into the current configuration. You should override the existing file.

```
user@host#
load override /var/tmp/filename
load complete
```

3. Commit the file.

```
user@host# commit
commit complete
```

4. Exit the CLI configuration mode.

```
user@host# exit
user@host>
```

5. Back up Junos OS.

   After you have installed the software on the router, committed the configuration, and are satisfied that the new configuration is successfully running, issue the **request system snapshot** command to back up the new software to the **/altconfig** file system. If you do not issue the **request system snapshot** command, the configuration on the alternate boot drive will be out of sync with the configuration on the primary boot drive.

   The **request system snapshot** command causes the root file system to be backed up to **/altroot**, and **/config** to be backed up to **/altconfig**. The root and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router's hard disk or solid-state drive (SSD).

Reverting to the Default Factory Configuration

If for any reason the current active configuration fails, you can revert to the default factory configuration. The default factory configuration contains the basic configuration settings. This is the first configuration of the switch, and it is loaded when the switch is first installed and powered on.

The **load factory default** command is a standard Junos OS configuration command. This configuration command replaces the current active configuration with the default factory configuration.

To revert the switch to the rescue configuration:

1. [edit]
   user@switch# **load factory-default**
   [edit]
   user@switch# **delete system commit factory-settings**
   [edit]
   user@switch# **commit**

Related Documentation

- *Understanding Configuration Files*
- *Loading a Previous Configuration File*
- Reverting to the Rescue Configuration on page 249

Reverting to the Default Factory Configuration by Using the request system zeroize Command

The **request system zeroize** command is a standard Junos OS operational mode command that removes all configuration information and resets all key values. The operation unlinks all user-created data files, including customized configuration and log files, from their directories. The switch then reboots and reverts to the factory-default configuration.

To completely erase user-created data so that it is unrecoverable, use the **request system zeroize media** command.

CAUTION: **Before issuing request system zeroize, use the request system snapshot command to back up the files currently used to run the switch to a secondary device.**

To revert to the factory-default configuration by using the **request system zeroize** command:

1. `user@switch>` **request system zeroize**
   ```
   warning: System will be rebooted and may not boot without configuration
   Erase all data, including configuration and log files? [yes,no] (yes)
   ```
2. Type **yes** to remove configuration and log files and revert to the factory default configuration.

3. Complete the initial configuration of the switch.

Related Documentation

- request system zeroize on page 406

Reverting to the Rescue Configuration

If someone inadvertently commits a configuration that denies management access to a device and the console port is not accessible, you can overwrite the invalid configuration and replace it with the rescue configuration. The rescue configuration is a previously committed, valid configuration.

To revert the switch to the rescue configuration:

1. Enter the **load override** command.

   [edit]
   user@switch# **load override** *filename*

2. Commit your changes.

   [edit]
   user@switch# **commit** *filename*

Related Documentation

- *Setting or Deleting the Rescue Configuration*
- Reverting to the Default Factory Configuration on page 248
- *Configuration File Terms*

CHAPTER 11

Reinstalling Software

Checklist for Reinstalling Junos OS

Table 27 on page 251 provides links and commands for reinstalling Junos OS.

Table 27: Checklist for Reinstalling Junos OS

Tasks	Command or Action
Before You Reinstall Junos OS	
1. Log the Software Version Information on page 253	**show version | save *filename***

Table 27: Checklist for Reinstalling Junos OS *(continued)*

Tasks	Command or Action
2. Log the Hardware Version Information on page 254	show chassis hardware | save *filename*
3. Log the Chassis Environment Information on page 255	show chassis environment | save *filename*
4. Log the System Boot-Message Information on page 256	show system boot-messages | save *filename*
5. Log the Active Configuration on page 258	show configuration | save *filename*
6. Log the Interfaces on the Router on page 258	show interface terse | save *filename*
7. Log the BGP, IS-IS, and OSPF Adjacency Information on page 259	show bgp summary | save *filename* show isis adjacency brief | save *filename* show ospf neighbor brief | save *filename*
8. Log the System Storage Information on page 260	show system storage | save *filename*
9. Back Up the Currently Running and Active File System on page 261	request system snapshot
10.	http://www.juniper.net/support
"Reinstall Junos OS" on page 261	Insert the floppy and reboot the system.
"Reconfigure Junos OS" on page 262	
1. Configure Host Names, Domain Names, and IP Addresses on page 262	Log in as root. Start the CLI. Enter configuration mode: configure set system host-name *host-name* set system domain-name *domain-name* set interfaces fxp0 unit 0 family inet address *address/prefix-length* set system backup-router *address* set system name-server *address*
2. Configuring the Root Password on page 264	set system root-authentication plain-text-password set system root-authentication encrypted-password password set system root-authentication ssh-rsa key commit exit
3. Check Network Connectivity on page 265	ping *address*
4. Copy Backup Configurations to the Router on page 266	file copy var/tmp configure [edit] load merge /config/*filename* or load replace /config/*filename* [edit] commit

Table 27: Checklist for Reinstalling Junos OS *(continued)*

Tasks	Command or Action
"After You Reinstall Junos OS" on page 270	
1. Compare Information Logged Before and After the Reinstall on page 270	show version | save *filename* show chassis hardware | save *filename* show chassis environment | save *filename* show system boot-messages | save *filename* show configuration | save *filename* show interfaces terse | save *filename* show bgp summary show isis adjacency brief show ospf neighbor brief | save *filename* show system storage | save *filename*
2. Back Up the New Software on page 271	request system snapshot

Log the Software Version Information

Action To log the Junos OS version information, use the following Junos OS CLI operational mode command:

```
user@host> show version | save filename
```

Sample Output

```
user@host> show version | save test
Wrote 39 lines of output to 'test'

user@host> show version
Hostname:  my-router.net
Model: m10
JUNOS Base OS boot [5.0R5]
JUNOS Base OS Software Suite [5.0R5]
JUNOS Kernel Software Suite [5.0R5]
JUNOS Routing Software Suite [5.0R5]
JUNOS Packet Forwarding Engine Support [5.0R5]
JUNOS Crypto Software Suite [5.0R5]
JUNOS Online Documentation [5.0R5]
KERNEL 5.0R5 #0 built by builder on 2002-03-02 05:10:28 UTC
MGD release 5.0R5 built by builder on 2002-03-02 04:45:32 UTC
CLI release 5.0R5 built by builder on 2002-03-02 04:44:22 UTC
CHASSISD release 5.0R5 built by builder on 2002-03-02 04:43:37 UTC
DCD release 5.0R5 built by builder on 2002-03-02 04:42:47 UTC
RPD release 5.0R5 built by builder on 2002-03-02 04:46:17 UTC
SNMPD release 5.0R5 built by builder on 2002-03-02 04:52:26 UTC
MIB2D release 5.0R5 built by builder on 2002-03-02 04:45:37 UTC
APSD release 5.0R5 built by builder on 2002-03-02 04:43:31 UTC
VRRPD release 5.0R5 built by builder on 2002-03-02 04:52:34 UTC
ALARMD release 5.0R5 built by builder on 2002-03-02 04:43:24 UTC
PFED release 5.0R5 built by builder on 2002-03-02 04:46:06 UTC
CRAFTD release 5.0R5 built by builder on 2002-03-02 04:44:30 UTC
SAMPLED release 5.0R5 built by builder on 2002-03-02 04:52:20 UTC
ILMID release 5.0R5 built by builder on 2002-03-02 04:45:21 UTC
BPRELAYD release 5.0R5 built by builder on 2002-03-02 04:42:41 UTC
RMOPD release 5.0R5 built by builder on 2002-03-02 04:46:11 UTC
jkernel-dd release 5.0R5 built by builder on 2002-03-02 04:41:07 UTC
jroute-dd release 5.0R5 built by builder on 2002-03-02 04:41:21 UTC
jdocs-dd release 5.0R5 built by builder on 2002-03-02 04:39:11 UTC
```

Meaning The sample output shows the hostname, router model, and the different Junos OS packages, processes, and documents.

Log the Hardware Version Information

Purpose You should log hardware version information in the rare event that a router cannot successfully reboot and you cannot obtain the Routing Engine serial number. The Routing Engine serial number is necessary for Juniper Networks Technical Assistance Center (JTAC) to issue a return to manufacturing authorization (RMA). Without the Routing Engine serial number, an onsite technician must be dispatched to issue the RMA.

Action To log the router chassis hardware version information, use the following Junos OS CLI operational mode command:

user@host> **show chassis hardware | save** ***filename***

Sample Output The output for the M-series routers varies depending on the chassis components of each router. All routers have a chassis, midplanes or backplanes, power supplies, and Flexible

PIC Concentrators (FPCs). Refer to the hardware guides for information about the different chassis components.

```
user@host> show chassis hardware | save test
Wrote 43 lines of output to 'test'

user@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                101               M160
Midplane         REV 02   710-001245   S/N AB4107
FPM CMB          REV 01   710-001642   S/N AA2911
FPM Display      REV 01   710-001647   S/N AA2999
CIP              REV 02   710-001593   S/N AA9563
PEM 0            Rev 01   740-001243   S/N KJ35769       DC
PEM 1            Rev 01   740-001243   S/N KJ35765       DC
PCG 0            REV 01   710-001568   S/N AA9794
PCG 1            REV 01   710-001568   S/N AA9804
Host 1                                 da000004f8d57001  teknor
MCS 1            REV 03   710-001226   S/N AA9777
SFM 0 SPP        REV 04   710-001228   S/N AA2975
SFM 0 SPR        REV 02   710-001224   S/N AA9838        Internet Processor I
SFM 1 SPP        REV 04   710-001228   S/N AA2860
SFM 1 SPR        REV 01   710-001224   S/N AB0139        Internet Processor I
FPC 0            REV 03   710-001255   S/N AA9806        FPC Type 1
  CPU            REV 02   710-001217   S/N AA9590
  PIC 1          REV 05   750-000616   S/N AA1527        1x OC-12 ATM, MM
  PIC 2          REV 05   750-000616   S/N AA1535        1x OC-12 ATM, MM
  PIC 3          REV 01   750-000616   S/N AA1519        1x OC-12 ATM, MM
FPC 1            REV 02   710-001611   S/N AA9523        FPC Type 2
  CPU            REV 02   710-001217   S/N AA9571
  PIC 0          REV 03   750-001900   S/N AA9626        1x STM-16 SDH, SMIR
  PIC 1          REV 01   710-002381   S/N AD3633        2x G/E, 1000 BASE-SX
FPC 2                                                    FPC Type OC192
  CPU            REV 03   710-001217   S/N AB3329
  PIC 0          REV 01                                  1x OC-192 SM SR-2
```

Meaning The sample output shows the hardware inventory for an M160 router with a chassis serial number of 101. For each component, the output shows the version number, part number, serial number, and description.

Log the Chassis Environment Information

Action To log the router chassis environment information, use the following Junos OS CLI operational mode command:

user@host> **show chassis environment | save** ***filename***

Sample Output The following example shows output from the **show chassis environment** command for an M5 router:

```
user@m5-host> show chassis environment | save test
Wrote 14 lines of output to 'test'

user@m5-host> show chassis environment
Class Item                  Status     Measurement
Power Power Supply A        OK
      Power Supply B        OK
Temp  FPC Slot 0            OK         32 degrees C / 89 degrees F
```

```
      FEB                    OK         31 degrees C / 87 degrees F
      PS Intake              OK         26 degrees C / 78 degrees F
      PS Exhaust             OK         31 degrees C / 87 degrees F
Fans  Left Fan 1             OK         Spinning at normal speed
      Left Fan 2             OK         Spinning at normal speed
      Left Fan 3             OK         Spinning at normal speed
      Left Fan 4             OK         Spinning at normal speed
```

Meaning The sample output shows the environmental information about the router chassis, including the temperature and information about the fans, power supplies, and Routing Engine.

Log the System Boot-Message Information

Action To log the system boot-message information, use the following Junos OS CLI operational mode command:

user@host> **show system boot-messages | save** ***filename***

Sample Output

```
user@host> show system boot-messages | save test
Wrote 80 lines of output to 'test'

user@host> show system boot-messages
Copyright (c) 1992-1998 FreeBSD Inc.
Copyright (c) 1996-2000 Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
        The Regents of the University of California.  All rights reserved.

JUNOS 4.1-20000216-Zf8469 #0: 2000-02-16 12:57:28 UTC

tlim@single.juniper.net:/p/build/20000216-0905/4.1/release_kernel/sys/compile/GENERIC
CPU: Pentium Pro (332.55-MHz 686-class CPU)
  Origin = "GenuineIntel"  Id = 0x66a  Stepping=10

Features=0x183f9ff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,SEP,MTRR,PGE,MCA,CMOV,<b16>,<b17>,MMX,<b24>>
Teknor CPU Card Recognized
real memory  = 805306368 (786432K bytes)
avail memory = 786280448 (767852K bytes)
Probing for devices on PCI bus 0:
chip0 <generic PCI bridge (vendor=8086 device=7192 subclass=0)> rev 3 class 60000
 on pci0:0:0
chip1 <Intel 82371AB PCI-ISA bridge> rev 1 class 60100 on pci0:7:0
chip2 <Intel 82371AB IDE interface> rev 1 class 10180 on pci0:7:1
chip3 <Intel 82371AB USB interface> rev 1 class c0300 int d irq 11 on pci0:7:2
smb0 <Intel 82371AB SMB controller> rev 1 class 68000 on pci0:7:3
pcic0 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int a irq 15 on pci0:13:0
TI1131 PCI Config Reg: [pci only][FUNC0 pci int]
pcic1 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int b irq 12 on pci0:13:1
TI1131 PCI Config Reg: [pci only][FUNC1 pci int]
fxp0 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 12 on
 pci0:16:0
chip4 <generic PCI bridge (vendor=1011 device=0022 subclass=4)> rev 4 class 60400
 on pci0:17:0
fxp1 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on
 pci0:19:0
Probing for devices on PCI bus 1:mcs0 <Miscellaneous Control Subsystem> rev 12
class ff0000 int a irq 12 on pci1:13:0
fxp2 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on
 pci1:14:0
Probing for devices on the ISA bus:
sc0 at 0x60-0x6f irq 1 on motherboard
sc0: EGA color <16 virtual consoles, flags=0x0>
ed0 not found at 0x300
ed1 not found at 0x280
ed2 not found at 0x340
psm0 not found at 0x60
sio0 at 0x3f8-0x3ff irq 4 flags 0x20010 on isa
sio0: type 16550A, console
sio1 at 0x3e8-0x3ef irq 5 flags 0x20000 on isa
sio1: type 16550A
sio2 at 0x2f8-0x2ff irq 3 flags 0x20000 on isa
sio2: type 16550A
pcic0 at 0x3e0-0x3e1 on isa
PC-Card ctlr(0) TI PCI-1131 [CardBus bridge mode] (5 mem & 2 I/O windows)
pcic0: slot 0 controller I/O address 0x3e0
npx0 flags 0x1 on motherboard
npx0: INT 16 interface
fdc0: direction bit not set
```

```
fdc0: cmd 3 failed at out byte 1 of 3
fdc0 not found at 0x3f0
wdc0 at 0x1f0-0x1f7 irq 14 on isa
wdc0: unit 0 (wd0): <SunDisk SDCFB-80>, single-sector-i/o
wd0: 76MB (156672 sectors), 612 cyls, 8 heads, 32 S/T, 512 B/S
wdc0: unit 1 (wd1): <IBM-DCXA-210000>
wd1: 8063MB (16514064 sectors), 16383 cyls, 16 heads, 63 S/T, 512 B/S
wdc1 not found at 0x170
wdc2 not found at 0x180
ep0 not found at 0x300
fxp0: Ethernet address 00:a0:a5:12:05:5a
fxp1: Ethernet address 00:a0:a5:12:05:59
fxp2: Ethernet address 02:00:00:00:00:01
swapon: adding /dev/wd1s1b as swap device
Automatic reboot in progress...
/dev/rwd0s1a: clean, 16599 free (95 frags, 2063 blocks, 0.1% fragmentation)
/dev/rwd0s1e: clean, 9233 free (9 frags, 1153 blocks, 0.1% fragmentation)
/dev/rwd0s1a: clean, 16599 free (95 frags, 2063 blocks, 0.1% fragmentation)
/dev/rwd1s1f: clean, 4301055 free (335 frags, 537590 blocks, 0.0% fragmentation)
```

Meaning The sample output shows the initial messages generated by the system kernel upon boot. This is the content of the **/var/run/dmesg.boot** file.

Log the Active Configuration

Action To log the active configuration on the router, use the following Junos OS CLI operational mode command:

user@host> **show configuration | save** ***filename***

Sample Output

```
user@host> show configuration | save test
Wrote 4076 lines of output to 'test'

user@host> show configuration
system {
host-name lab8;
domain-name juniper.net;
backup-router 10.1.1.254;
    time-zone America/Los_Angeles;
default-address-selection;
    dump-on-panic;
name-server {
[...Output truncated...]
```

Meaning The sample output shows the configuration currently running on the router, which is the last committed configuration.

Log the Interfaces on the Router

Action To log the interfaces on the router, use the following Junos OS CLI operational mode command:

user@host> **show interface terse | save** ***filename***

Sample Output

```
user@host> show interfaces terse | save test
Wrote 81 lines of output to 'test'

user@host> show interfaces terse
Interface       Admin Link Proto Local             Remote
at-1/3/0        up    up
at-1/3/0.0      up    up   inet  1.0.0.1           --> 1.0.0.2
                           iso
fxp0            up    up
fxp0.0          up    up   inet  10.168.5.59/24
gre             down  up
ipip            down  up
lo0             up    up
lo0.0           up    up   inet  127.0.0.1         --> 0/0
                          iso 47.0005.80ff.f800.0000.0108.0001.1921.6800.5059.00
so-1/2/0        up    down
so-1/2/1        down  down
so-1/2/2        down  down
so-1/2/3        down  down
so-2/0/0        up    up
so-2/0/0.0      up    up   inet  1.2.3.4           --> 1.2.3.5
                           iso
[...Output truncated...]
```

Meaning The sample output displays summary information about the physical and logical interfaces on the router.

Log the BGP, IS-IS, and OSPF Adjacency Information

Purpose The following commands log useful information about Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF) protocols. If you have other protocols installed, such as Multiprotocol Label Switching (MPLS), Resource Reservation Protocol (RSVP), or Protocol Independent Multicast (PIM), you also might log summary information for them.

Action To log the protocol peer information, use the following Junos OS CLI operational mode commands:

```
user@host> show bgp summary | save filename
user@host> show isis adjacency brief | save filename
user@host> show ospf neighbor brief | save filename
```

Sample Output 1

```
user@host> show bgp summary | save test
Wrote 45 lines of output to 'test'

user@host> show bgp summary
Groups: 1 Peers: 1 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 4          4          0          0          0          0
Peer               AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Damped..
9.9.3.1             2       2627       2628       0       0    21:50:12 4/4/0
             0/0/0
```

Sample Output 2

```
user@host> show isis adjacency brief | save test
Wrote 7 lines of output to 'test'

user@host> show isis adjacency brief
IS-IS adjacency database:
Interface  System         L State        Hold (secs) SNPA
so-1/0/0.0 1921.6800.5067 2 Up                    13
so-1/1/0.0 1921.6800.5067 2 Up                    25
so-1/2/0.0 1921.6800.5067 2 Up                    20
so-1/3/0.0 1921.6800.5067 2 Up                    19
so-2/0/0.0 1921.6800.5066 2 Up                    19
so-2/1/0.0 1921.6800.5066 2 Up                    17
so-2/2/0.0 1921.6800.5066 2 Up                    20
so-2/3/0.0 1921.6800.5066 2 Up                    20
so-5/0/0.0 ranier         2 Up                    17
```

Sample Output 3

```
user@host> show ospf neighbor brief | save test
Wrote 10 lines of output to 'test'

user@host> show ospf neighbor brief
  Address         Intf               State      ID              Pri  Dead
10.168.254.225   fxp3.0              2Way      10.250.240.32    128   36
10.168.254.230   fxp3.0              Full      10.250.240.8     128   38
10.168.254.229   fxp3.0              Full      10.250.240.35    128   33
10.1.1.129       fxp2.0              Full      10.250.240.12    128   37
10.1.1.131       fxp2.0              Full      10.250.240.11    128   38
10.1.2.1         fxp1.0              Full      10.250.240.9     128   32
10.1.2.81        fxp0.0              Full      10.250.240.10    128   33
```

Meaning Sample output 1 displays summary information about BGP and its neighbors. Sample output 2 displays information about IS-IS neighbors. Sample output 3 displays information about all OSPF neighbors.

Log the System Storage Information

Action To log the system storage statistics for the amount of free disk space in the router's file system, use the following Junos OS CLI operational mode command:

user@host> **show system storage | save *filename***

Sample Output

```
user@host> show system storage | save test
Wrote 14 lines of output to 'test'

user@host> show system storage
Filesystem  1K-blocks     Used    Avail Capacity  Mounted on
/dev/ad0s1a     65687    26700    33733    44%    /
devfs              16       16        0   100%    /dev/
/dev/vn1         9310     9310        0   100%    /packages/mnt/jbase
/dev/vn2         8442     8442        0   100%    /packages/mnt/jkernel-5.0R5.1
/dev/vn3        11486    11486        0   100%    /packages/mnt/jpfe-5.0R5.1
/dev/vn4         5742     5742        0   100%    /packages/mnt/jroute-5.0R5.1
/dev/vn5         1488     1488        0   100%    /packages/mnt/jcrypto-5.0R5.1
/dev/vn6          792      792        0   100%    /packages/mnt/jdocs-5.0R5.1
mfs:2373      1015815        3   934547     0%    /tmp
/dev/ad0s1e     25263       11    23231     0%    /config
procfs              4        4        0   100%    /proc
/dev/ad1s1f   9825963  1811085  7228801    20%    /var
```

Meaning The sample output displays statistics about the amount of free disk space in the router's file system. Values are displayed in 1024-byte (1-KB) blocks.

Back Up the Currently Running and Active File System

Action To back up the currently running and active file system so that you can recover to a known, stable environment in case there is a problem during the reinstall, use the following Junos OS CLI operational mode command:

```
user@host> request system snapshot
```

Sample Output

```
user@host> request system snapshot
umount: /altroot: not currently mounted
Copying / to /altroot.. (this may take a few minutes)
umount: /altconfig: not currently mounted
Copying /config to /altconfig.. (this may take a few minutes)
The following filesystems were archived: / /config
```

Meaning The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's internal flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.

NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Reinstall Junos OS

Action To reinstall Junos OS, follow these steps:

1. Insert the removable medium (boot floppy) into the router.
2. Reboot the router, either by power-cycling it or by issuing the **request system reboot** command from the CLI.
3. At the following prompt, type **y**:

   ```
   WARNING: The installation will erase the contents of your disk. Do you wish
   to continue (y/n)?
   ```

   The router copies the software from the removable medium onto your system, occasionally displaying status messages. This can take up to 10 minutes.
4. Remove the removable medium when prompted.

   The router reboots from the primary boot device on which the software is installed. When the reboot is complete, the router displays the login prompt.

Reconfigure Junos OS

Purpose After you have reinstalled the software, you must copy the router's configuration files back to the router. (You also can configure the router from scratch, as described in *Junos System Basics Configuration Guide*) However, before you can copy the configuration files, you must establish network connectivity.

To reconfigure the software, follow these steps:

1. Configure Host Names, Domain Names, and IP Addresses on page 262
2. Configuring the Root Password on page 264
3. Check Network Connectivity on page 265
4. Copy Backup Configurations to the Router on page 266

Configure Host Names, Domain Names, and IP Addresses

Action To configure the machine name, domain name, and various addresses, follow these steps:

1. Log in as **root**. There is no password.
2. Start the CLI:

   root# **cli**
   root@>
3. Enter configuration mode:

   cli> **configure**
   [edit]
   root@#
4. Configure the name of the machine. If the name includes spaces, enclose the entire name in quotation marks (" "):

   [edit]
   root@# **set system host-name** *host-name*
5. Configure the machine's domain name:


```
[edit]
root@# set system domain-name domain-name
```

6. Configure the IP address and prefix length for the router's management Ethernet interface:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address / prefix-length
```

7. Configure the IP address of a default router. This system is called the backup router because it is used only while the routing protocol process is not running.

```
[edit]
root@# set system backup-router address
```

8. Configure the IP address of a Domain Name Server (DNS) server:

```
[edit]
root@# set system name-server address
```

Configuring the Root Password

Junos OS is preinstalled on the router. When the router is powered on, it is ready to be configured. Initially, you log in as the user **root** with no password. The root directory of a UNIX device is the entry point to all other folders and files on that device. As a result, access to the root directory is restricted by default to a predefined user account known as the root user. The root user (also referred to as superuser) has unrestricted access and full permissions within the system. The expression “log in as root” is commonly used when an action requires the user to log into the device as the root user. Junos OS requires configuration of the root password before it accepts a commit operation. On a new device, the root password must always be a part of the configuration submitted with your initial commit.

To set the root password, you have several options: enter a clear-text password that Junos OS encrypts, enter a password that is already encrypted, or enter a secure shell (ssh) public key string.

Optionally, instead of configuring the root password at the **[edit system]** hierarchy level, you can use a configuration group, as shown in this procedure. This is a recommended best practice for configuring the root password. This procedure uses a group called **global** as an example.

To set the root password:

1. Use one of the following methods to configure the root password.

   - To enter a clear-text password that the system encrypts for you, use the following command to set the root password:

     [edit groups global system]
     root@# **set root-authentication plain-text-password**
     New Password: ***type password here***
     Retype new password: *retype password here*

     If you use a clear-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are hidden and marked as **## SECRET-DATA** in the configuration.

   - To enter a password that is already encrypted, use the following command to set the root password:

     CAUTION: Do not use the **encrypted-password** option unless the password is *already* encrypted, and you are entering the encrypted version of the password.

     If you accidentally configure the **encrypted-password** option with a clear-text password or with blank quotation marks (" "), you will not be able to log in to the device as root, and you will need to complete the root password recovery process.

     [edit groups global system]
     root@# **set root-authentication encrypted-password** ***password***

   - To enter an SSH public string, use the following command to set the root password:

     [edit groups global system]
     root@# **set root-authentication (ssh-dsa | ssh-ecdsa | ssh-rsa*key***

2. (Optional) Strengthen security by only allowing root access from the console port.

   [edit groups global system]
   root@# **set services ssh root-login deny**

3. If you used a configuration group, apply the configuration group, substituting **global** with the appropriate group name.

   [edit]
   user@host# **set apply-groups global**

4. Commit the changes.

   root@# **commit**

Check Network Connectivity

Purpose Establish that the router has network connectivity.

Action To check that the router has network connectivity, issue a **ping** command to a system on the network:

```
root@> ping address
```

If there is no response, verify that there is a route to the ***address*** using the **show route** command. If the address is outside your **fxp0** subnet, add a static route. Once the backup configuration is loaded and committed, the static route is no longer needed and should be deleted.

Copy Backup Configurations to the Router

Action To copy backup configurations to the router, follow these steps:

1. To copy the existing configuration and any backup configurations back onto the router, use the **file copy** command. Place the files in the **/var/tmp** directory.

   ```
   user@host> file copy var/tmp/filename
   ```

2. Load and activate the desired configuration:

   ```
   root@> configure
   [edit]
   root@# load merge/config/filename or load replace/config/filename
   [edit]
   root@# commit
   ```

Configure Host Names, Domain Names, and IP Addresses

Action To configure the machine name, domain name, and various addresses, follow these steps:

1. Log in as **root**. There is no password.
2. Start the CLI:

   ```
   root# cli
   root@>
   ```

3. Enter configuration mode:

   ```
   cli> configure
   [edit]
   root@#
   ```

4. Configure the name of the machine. If the name includes spaces, enclose the entire name in quotation marks (" "):

   ```
   [edit]
   root@# set system host-name host-name
   ```

5. Configure the machine's domain name:

   ```
   [edit]
   root@# set system domain-name domain-name
   ```

6. Configure the IP address and prefix length for the router's management Ethernet interface:


```
[edit]
root@#   set interfaces fxp0 unit 0 family inet address address / prefix-length
```

7. Configure the IP address of a default router. This system is called the backup router because it is used only while the routing protocol process is not running.

```
[edit]
root@#  set system backup-router address
```

8. Configure the IP address of a Domain Name Server (DNS) server:

```
[edit]
root@# set system name-server  address
```

Configuring the Root Password

Junos OS is preinstalled on the router. When the router is powered on, it is ready to be configured. Initially, you log in as the user **root** with no password. The root directory of a UNIX device is the entry point to all other folders and files on that device. As a result, access to the root directory is restricted by default to a predefined user account known as the root user. The root user (also referred to as superuser) has unrestricted access and full permissions within the system. The expression “log in as root” is commonly used when an action requires the user to log into the device as the root user. Junos OS requires configuration of the root password before it accepts a commit operation. On a new device, the root password must always be a part of the configuration submitted with your initial commit.

To set the root password, you have several options: enter a clear-text password that Junos OS encrypts, enter a password that is already encrypted, or enter a secure shell (ssh) public key string.

Optionally, instead of configuring the root password at the **[edit system]** hierarchy level, you can use a configuration group, as shown in this procedure. This is a recommended best practice for configuring the root password. This procedure uses a group called **global** as an example.

To set the root password:

1. Use one of the following methods to configure the root password.

   - To enter a clear-text password that the system encrypts for you, use the following command to set the root password:

     [edit groups global system]
     root@# **set root-authentication plain-text-password**
     New Password: ***type password here***
     Retype new password: *retype password here*

     If you use a clear-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are hidden and marked as **## SECRET-DATA** in the configuration.

   - To enter a password that is already encrypted, use the following command to set the root password:

     CAUTION: Do not use the **encrypted-password** option unless the password is *already* encrypted, and you are entering the encrypted version of the password.

     If you accidentally configure the **encrypted-password** option with a clear-text password or with blank quotation marks (" "), you will not be able to log in to the device as root, and you will need to complete the root password recovery process.

     [edit groups global system]
     root@# **set root-authentication encrypted-password** ***password***

   - To enter an SSH public string, use the following command to set the root password:

     [edit groups global system]
     root@# **set root-authentication (ssh-dsa | ssh-ecdsa | ssh-rsa***key*

2. (Optional) Strengthen security by only allowing root access from the console port.

   [edit groups global system]
   root@# **set services ssh root-login deny**

3. If you used a configuration group, apply the configuration group, substituting **global** with the appropriate group name.

   [edit]
   user@host# **set apply-groups global**

4. Commit the changes.

   root@# **commit**

Related Documentation

- *Accessing a Junos OS Device the First Time*
- *Understanding User Accounts*
- *Recovering the Root Password*

Check Network Connectivity

Purpose Establish that the router has network connectivity.

Action To check that the router has network connectivity, issue a **ping** command to a system on the network:

```
root@> ping address
```

If there is no response, verify that there is a route to the ***address*** using the **show route** command. If the address is outside your **fxp0** subnet, add a static route. Once the backup configuration is loaded and committed, the static route is no longer needed and should be deleted.

Copy Backup Configurations to the Router

Action To copy backup configurations to the router, follow these steps:

1. To copy the existing configuration and any backup configurations back onto the router, use the **file copy** command. Place the files in the **/var/tmp** directory.

   ```
   user@host> file copy var/tmp/filename
   ```

2. Load and activate the desired configuration:

   ```
   root@> configure
   [edit]
   root@# load merge/config/filename or load replace/config/filename
   [edit]
   root@# commit
   ```

After You Reinstall Junos OS

To verify that the new version of the Junos OS is running as expected after the reinstall, follow these steps:

1. Compare Information Logged Before and After the Reinstall on page 270
2. Back Up the New Software on page 271

Compare Information Logged Before and After the Reinstall

Purpose Compare the operation of the system before and after the reinstall to ensure that everything is working as expected.

Action To obtain system information, use the following commands:

```
user@host> show version
user@host> show chassis hardware
user@host> show chassis environment
user@host> show system boot-messages
user@host> show configuration
user@host> show interface terse
user@host> show bgp summary
```



```
user@host> show isis adjacency brief
user@host> show ospf neighbor brief
user@host> show system storage
```

Compare the information from these commands with the information you obtained before the reinstall.

Back Up the New Software

Purpose After a week or so, when you are satisfied that the new software is running successfully, we recommend that you back up the reinstalled software.

Action To back up the reinstalled software, use the following Junos OS CLI operational mode command:

```
user@host> request system snapshot
```

The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's internal flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.

NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Compare Information Logged Before and After the Reinstall

Purpose Compare the operation of the system before and after the reinstall to ensure that everything is working as expected.

Action To obtain system information, use the following commands:

```
user@host> show version
user@host> show chassis hardware
user@host> show chassis environment
user@host> show system boot-messages
user@host> show configuration
user@host> show interface terse
user@host> show bgp summary
user@host> show isis adjacency brief
user@host> show ospf neighbor brief
user@host> show system storage
```

Compare the information from these commands with the information you obtained before the reinstall.

Back Up the New Software

Purpose After a week or so, when you are satisfied that the new software is running successfully, we recommend that you back up the reinstalled software.

Action To back up the reinstalled software, use the following Junos OS CLI operational mode command:

```
user@host> request system snapshot
```

The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's internal flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.

NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Reinstalling the Single-Root Partition on SRX Series Devices

Junos OS Release 9.6 and earlier is not compatible with the dual-root partitioning scheme. These releases can only be installed if the media is reformatted with single-root partitioning. Any attempt to install Junos OS Release 9.6 or earlier on a device with dual-root partitioning without reformatting the media will fail with an error. You must install the Junos OS Release 9.6 or earlier image from the boot loader using a TFTP server or USB storage device.

NOTE: You do not need to reinstall the earlier version of the boot loader if you are installing the Junos OS Release 9.6.

You cannot install a Junos OS Release 9.6 or earlier package on a system with dual-root partitioning using the Junos OS CLI or J-Web. If this is attempted, an error will be returned.

You can install the Junos OS Release 9.6 (9.6R3 and 9.6R4 [only]) on a system with dual-root partitioning using **request system software add** command with **partition** option.

To reinstall the single-root partition:

1. Enter the request system software add partition command to install the previous Junos OS version (9.6R3 and 9.6R4):

   user@host>request system software add partition

2. Reboot the device

   user@host>request system reboot

   The previous software version gets installed after rebooting the device.

NOTE: Using the **request system software add** CLI command with the **partition** option to install Junos OS Release 9.6 (9.6R3 and 9.6R4) reformats the media with single-root partitioning. This process erases the dual-root partitioning scheme from the system, so the benefits of dual-root partitioning will no longer be available.

Related Documentation

- Dual-Root Partitioning Scheme on SRX Series Devices on page 97
- Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 71
- *Installation and Upgrade Guide*

CHAPTER 12

Downgrading Software

Example: Downgrading Junos OS on J Series and SRX Series Devices

This example shows how to downgrade Junos OS on the SRX Series devices and J Series Routers.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

When you upgrade your software, the device creates a backup image of the software that was previously installed in addition to installing the requested software upgrade.

To downgrade the software, you can revert to the previous image using the backup image. You can use this method to downgrade to only the software release that was installed on the device before the current release. To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release. This example returns software to the previous Junos OS version.

NOTE: **This procedure applies only to downgrading from one Junos OS software release to another or from one Junos OS services release to another.**

Configuration

CLI Quick Configuration

To quickly downgrade Junos OS on SRX Series devices, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>
request system software rollback
request system reboot
```

GUI Step-by-Step Procedure

To downgrade Junos OS on SRX Series devices:

1. In the J-Web user interface, select **Maintain>Software>Downgrade**. The image of the previous version (if any) appears on this page.

   NOTE: **After you perform this operation, you cannot undo it.**

2. Select **Downgrade** to downgrade to the previous version of the software or **Cancel** to cancel the downgrade process.
3. Click **Maintain>Reboot** from the J-Web user interface to reboot the device.

   NOTE: **To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.**

4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To downgrade Junos OS on SRX Series devices:

1. From operational mode, return to the previous Junos OS version.

   user@host> **request system software rollback**

2. Reboot the device.

   user@host> **request system reboot**

   The device is now running the previous version of Junos OS. To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the Junos OS Downgrade Installation on page 277

Verifying the Junos OS Downgrade Installation

Purpose Verify that the Junos OS downgrade was installed.

Action From operational mode, enter the **show system** command.

Related Documentation

- Configuring Boot Devices for J Series and SRX Series Devices on page 216
- Understanding Junos OS Upgrades for J Series and SRX Series Devices on page 188
- Example: Installing Junos OS Upgrade Packages on J Series and SRX Series Devices on page 196
- Restarting and Halting J Series and SRX Series Devices on page 279
- *Installation and Upgrade Guide*

CHAPTER 13

Rebooting or Halting Software Processes on a Device

Restarting and Halting J Series and SRX Series Devices

This topic includes the following sections:

Example: Rebooting J Series and SRX Series Devices

This example shows how to reboot a J Series device.

Requirements

Before rebooting the device, save and commit any Junos OS updates.

Overview

This example shows how to reboot a device fifty minutes from when you set the time from the internal media while sending a text message of 'stop' to all system users before the device reboots.

Configuration

- [xref target has no title]

CLI Quick Configuration

To quickly reboot a device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

For SRX Series devices, from operational mode, enter:

```
user@host> request system reboot at 5 in 50 media internal message stop
```

For J Series devices, from operational mode, enter:

```
user@host>request system reboot at 5 in 50 media usb message stop
```

GUI Step-by-Step Procedure

To reboot a device:

1. In the J-Web user interface, select **Maintain>Reboot**.
2. Select **Reboot in *50* minutes** to reboot the device fifty minutes from the current time.
3. Select the **internal** (for SRX Series devices) or **usb** (for J Series devices) boot device from the Reboot From Media list.
4. In the Message box, type **stop** as the message to display to any user on the device before the reboot occurs.
5. Click **Schedule**. The J-Web user interface requests confirmation to perform the reboot.
6. Click **OK** to confirm the operation.
   - If the reboot is scheduled to occur immediately, the device reboots. You cannot access J-Web until the device has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web login page.
   - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web user interface Reboot page.
7. Click **OK** to check your configuration and save it as a candidate configuration.
8. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To reboot a device:

From operational mode, schedule a reboot of the device to occur fifty minutes from when you set the time from the internal media while sending a text message of 'stop' to all system users before the device reboots.

For SRX Series devices, enter:

```
user@host> request system reboot at 5 in 50 media internal message stop
```

For J Series devices, enter:

```
user@host>request system reboot at 5 in 50 media usb message stop
```

Results From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the Device Reboot on page 281

Verifying the Device Reboot

Purpose Verify that the device rebooted.

Action From operational mode, enter the **show system** command.

Example: Halting J Series and SRX Series Devices

This example shows how to halt a device.

- Requirements on page 281
- Overview on page 281
- Configuration on page 281
- Verification on page 282

Requirements

Before halting the device, save and commit any Junos OS updates.

Overview

When the device is halted, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.

NOTE: If you cannot connect to the device through the console port, shut down the device by pressing and holding the power button on the front panel until the POWER LED turns off. After the device has shut down, you can power on the device by pressing the power button again. The POWER LED turns on during startup and remains steadily green when the device is operating normally.

This example shows how to halt the system and stop software processes on the device immediately.

Configuration

- [xref target has no title]

CLI Quick Configuration

To quickly halt a device immediately, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>request system halt at now
```

GUI Step-by-Step Procedure

To halt a device immediately:

1. In the J-Web user interface, select **Maintain>Reboot**.
2. Select **Halt Immediately**. After the software stops, you can access the device through the console port only.
3. Click **Schedule**. The J-Web user interface requests confirmation to halt.
4. Click **OK** to confirm the operation. If the device halts, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.
5. Click **OK** to check your configuration and save it as a candidate configuration.
6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To halt a device:

From operational mode, halt the SRX Series device immediately.

```
user@host> request system halt at now
```

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the Device Halt on page 282

Verifying the Device Halt

Purpose

Verify that the device halted.

Action

From operational mode, enter the **show system** command.

Bringing Chassis Components Online and Offline on J Series and SRX Series Devices

You can use the **request** commands to bring all chassis components (except Power Entry Modules and fans) online and offline.

To bring chassis components online and offline, enter these **request chassis** commands:

```
user@host> request chassis <fru> slot <slot#> pic <pic#> offline
user@host> request chassis <fru> slot <slot#> pic <pic#> online
```

Where **<*fru*>** in the request chassis command can be any of the following (for SRX Series devices):

- **cluster**—Changes the chassis cluster status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.

Where **<*fru*>** in the request chassis command can be any of the following (for J Series devices):

- **cb**—Changes the control board status.
- **cluster**—Changes the chassis cluster status.
- **fabric**—Changes the fabric status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.
- **fpm**—Changes the craft interface status.
- **pic**—Changes the physical interface card status.
- **routing-engine—**Changes the routing engine status.

To bring specific pic and the corresponding fpc slot online, from operational mode enter the following **request chassis** command:

```
user@host> request chassis pic pic-slot 1 fpc-slot 1 online
```

Restarting the Chassis on J Series and SRX Series Devices

You can restart the chassis using the **restart chassis-control** command with the following options:

- To restart the process gracefully:

  user@host> restart chassis-control gracefully

- To restart the process immediately:

  user@host> restart chassis-control immediately

- To restart the process softly:

  user@host> restart chassis-control soft

Rebooting or Halting the EX Series Switch (J-Web Procedure)

You can use the J-Web interface to schedule a reboot or to halt the switching platform.

To reboot or halt the switching platform by using the J-Web interface:

1. In the J-Web interface, select **Maintain** > **Reboot**.
2. Select one:
   - **Reboot Immediately**—Reboots the switching platform immediately.
   - **Reboot in *number of* minutes**—Reboots the switch in the number of minutes from now that you specify.
   - **Reboot when the system time is *hour:minute*** —Reboots the switch at the absolute time that you specify, on the current day. You must select a 2-digit hour in 24-hour format and a 2-digit minute.
   - **Halt Immediately**— Stops the switching platform software immediately. After the switching platform software has stopped, you can access the switching platform through the console port only.
3. (Optional) In the Message box, type a message to be displayed to any users on the switching platform before the reboot occurs.
4. Click **Schedule**. The J-Web interface requests confirmation to perform the reboot or halt.
5. Click **OK** to confirm the operation.
   - If the reboot is scheduled to occur immediately, the switch reboots. You cannot access the J-Web interface until the switch has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web interface login page.
   - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web interface Reboot page.
   - If the switch is halted, all software processes stop and you can access the switching platform through the console port only. Reboot the switch by pressing any key on the keyboard.

Related Documentation

- *Starting the J-Web Interface*

PART 3

Installing and Managing Software Licenses

CHAPTER 14

Software License Overview

Junos OS Feature Licenses

Some Junos OS software features require a license to activate the feature. To enable a licensed feature, you need to purchase, install, manage, and verify a license key that corresponds to each licensed feature. To conform to Junos OS feature licensing requirements, you must purchase one license per feature per device. The presence of the appropriate software license key on your device determines whether you are eligible to configure and use the licensed feature.

To speed deployment of licensed features, Junos OS software implements an honor-based licensing structure and provides you with a 30-day grace period to use a licensed feature without a license key installed. The grace period begins when you configure the feature and your device uses the licensed feature for the first time, but not necessarily when you install the license. After the grace period expires, the system generates system log messages saying that the feature requires a license. To clear the error message and use the licensed feature properly, you must install and verify the required license.

For information about how to purchase software licenses, contact your Juniper Networks sales representative.

Related Documentation

- License Enforcement on page 287
- Junos OS Feature License Keys on page 288
- Software Feature Licenses on page 292
- Verifying Junos OS License Installation on page 316

License Enforcement

For features or scaling levels that require a license, you must install and properly configure the license to meet the requirements for using the licensable feature or scale level. The

router or switch enables you to commit a configuration that specifies a licensable feature or scale without a license for a 30-day grace period. The grace period is a short-term grant that enables you to start using features in the pack or scale up to the system limits (regardless of the license key limit) without a license key installed. The grace period begins when the licensable feature or scaling level is actually used by the device (not when it is first committed). In other words, you can commit licensable features or scaling limits to the device configuration, but the grace period does not begin until the device uses the licensable feature or exceeds a licensable scaling level.

NOTE: Configurations might include both licensed and nonlicensed features. For these situations, the license is enforced up to the point where the license can be clearly distinguished. For example, an authentication-order configuration is shared by both Authentication, Authorization, and Accounting (AAA), which is licensed, and by Layer 2 Tunneling Protocol (L2TP), which is not licensed. When the configuration is committed, the device does not issue any license warnings, because it is not yet known whether AAA or L2TP is using the configuration. However, at runtime, the device checks for a license when AAA authenticates clients, but does not check when L2TP authenticates clients.

The device reports any license breach as a warning log message whenever a configuration is committed that contains a feature or scale limit usage that requires a license. Following the 30-day grace period, the device periodically reports the breach to syslog messages until a license is installed and properly configured on the device to resolve the breach.

NOTE: Successful commitment of a licensable feature or scaling configuration does not imply that the required licenses are installed or not required. If a required license is not present, the system issues a warning message after it commits the configuration.

Related Documentation

- Junos OS Feature Licenses on page 287
- Junos OS Feature License Keys on page 288
- Software Feature Licenses on page 292
- Verifying Junos OS License Installation on page 316

Junos OS Feature License Keys

Some Junos OS software features require a license to be activated. To enable each licensed feature, you must purchase, install, manage, and verify a license key that corresponds to the licensed feature.

Release-Tied License Keys and Upgrade Licenses on MX Series Routers

The Junos OS licensing infrastructure currently associates a license feature with attributes such as date, platform, and validity. In addition to these attributes, for MX Series routers running Junos OS Release 12.2 and later, a licensed feature can be associated with a release number at the time of generating the license key. This type of release-tied license key is used to validate a particular licensed feature while attempting a software upgrade. The upgrade process aborts if the release number in the license key is earlier than the Junos OS release number to which the system is being upgraded.

Additionally, an upgrade license key can be generated for a release-tied licensed feature. An upgrade license key is used for carrying forward a capacity license to the upgrade release. Although an upgrade license might be an acceptable license on the current release, it does not add to the existing capacity limit. The capacity added in the upgrade license key is valid for the upgrade software release only.

The release number embedded in the license key indicates the maximum release number up to which Junos OS can be upgraded.

As an example, assume that your system is running Junos OS Release 12.2 and is using the **scale-subscriber** licensed feature with a later release-tied upgrade license key installed. If you request a software upgrade to the later release of Junos OS, the software upgrade operation fails and the following error message is displayed:

```
mgd: error: No valid upgrade license found for feature 'scale-subscriber'.
Aborting Software upgrade.
Validation failed
```

In this example, to successfully upgrade to the later release of Junos OS, the release number included in the upgrade license key should be greater than or equal to the later release number. Also, you can perform software upgrades up to the previous release without any additional license keys to retain the existing scale limit.

NOTE:

When you install a release-tied license, the following apply:

- You can purchase an upgrade capacity license only if a base capacity license for the same scale-tier has already been generated or purchased.
- You cannot install an upgrade license if the capacity does not match any of the existing base capacity licenses on the system.
- The license installation fails when you install a lower release number license key on a higher software release number.
- A release-tied license can be installed on a Junos OS release number that is lower than or equal to the release number included in the license key. For example, a 12.2 license key is valid on Junos OS Release 12.1.
- An upgrade license is valid only on the target release number specified in the license key, but can be installed on an earlier Junos OS release. For example, a 4 K scale-tier upgrade license for Junos OS Release 12.2 can be installed on an earlier release, and the installed count of licenses remains unaltered.
- Release-tied licenses of the previous release are not deleted on upgrading Junos OS to a newer release version.

Licensable Ports on MX5, MX10, and MX40 Routers

Starting with Junos OS Release 12.2, license keys are available to enhance the port capacity on MX5, MX10, and MX40 routers up to the port capacity of an MX80 router. The MX5, MX10, and MX40 routers are derived from the modular MX80 chassis with similar slot and port assignments, and provide all functionality available on an MX80 router, but at a lower capacity. Restricting port capacity is achieved by making a set of MIC slots and ports licensable. MICs without a license are locked, and are unlocked or made usable by installing appropriate upgrade licenses.

The base capacity of a router is identified by the Ideeprom assembly ID (I2C ID), which defines the board type. However, the Junos OS licensing infrastructure allows the use of restricted ports without a license for a grace period of 30 days. After the grace period expires, the router reverts back to the base capacity if no upgrade license is purchased and installed for the locked ports. The I2C ID along with an upgrade license determine the final capacity of an MX5, MX10, or MX40 router.

The MX5, MX10, MX40, and MX80 routers support the following types of MICs:

- A built-in 10-Gigabit Ethernet MIC with four 10-Gigabit Ethernet ports
- Two front-pluggable MICs

A feature ID is assigned to every license upgrade for enhancing port capacity. Table 28 on page 291 displays the chassis types and their associated port capacity, I2C ID, base capacity, feature ID, feature name, and the final capacity after a license upgrade.

Table 28: Upgrade Licenses for Enhancing Port Capacity

Chassis Type	Port Capacity	I2C ID	Base Capacity	Feature ID and Feature Name	Upgrade Capacity
MX5	20G	0x556	Slot 1 • 1/MIC0	f1—MX5 to MX10 upgrade	Slot 1 and 2 • 1/MIC0 • 1/MIC1
MX10	40G	0x555	Slot 1 and 2 • 1/MIC0 • 1/MIC1	f2—MX10 to MX40 upgrade	Slot 2 and first 2 ports on Slot 0 • 1/MIC1 • First 2 ports on 0/MIC0
MX40	60G	0x554	Slot 1, SLot 2 and first 2 ports on Slot 0 • 1/MIC0 • 1/MIC1 • First 2 ports on 0/MIC0	f3—MX40 to MX80 upgrade	Slot 2 and all ports on Slot 0 • 1/MIC1 • All 4 ports on 0/MIC0

When installing an upgrade license for enhancing port capacity on MX5, MX10 and MX40 routers, consider the following:

- To upgrade an MX5 router to MX80 router capacity, licenses for all three features (f1, f2, f3) must be installed. All three features can be provided in a single license key.
- To upgrade an MX10 router to MX40 router capacity, installing a license key with f2 feature is sufficient.
- Non-applicable feature IDs in a license key reject the upgrade license. For example:
  - An f1 feature ID on an MX10 upgrade license key rejects the license.
  - Feature IDs f1 and f2 on an MX40 upgrade license key reject the entire license.

Port Activation on MX104 Routers

Starting with Junos OS Release 13.3, license keys are available to activate the ports on the MX104 router. MX104 routers have four built-in ports. By default, in the absence of valid licenses, all four built-in ports are deactivated. By installing licenses, you can activate any two of the four or all of the four built-in ports. For instance, you can install a license to activate the first two built-in ports (xe-2/0/0 and xe-2/0/1) or you can install a license to activate the next two built-in ports (xe-2/0/2 and xe-2/0/3). You can also install a license to activate all four built-in ports (xe-2/0/0, xe-2/0/1, xe-2/0/2, and xe-2/0/3). If you have already activated two of the built-in ports, you can install an additional license to activate the other two built-in ports on the MX104 router.

A feature ID is assigned to every license for activating the built-in ports on the MX104 router. The port license model with the feature ID is described in Table 29 on page 292.

Table 29: Port Activation License Model for MX104 Routers

Feature ID	Feature Name	Functionality
F1	MX104 2X10G Port Activate (0 and 1)	Ability to activate first two built-in ports (xe-2/0/0 and xe-2/0/1)
F2	MX104 2X10G Port Activate (2 and 3)	Ability to activate next two built-in ports (xe-2/0/2 and xe-2/0/3)

Both the features are also provided in a single license key for ease of use. To activate all four ports, you must either install the licenses for both the features listed in Table 29 on page 292 or the single license key for both features. If you install the single license key when feature IDs F1 and F2 are already installed, the license does not get rejected. Also, MX104 routers do not support the graceful license expiry policy. A graceful license expiry policy allows the use of a feature for a certain period of time (usually a grace period of 30 days), and reverts if the license for that feature is not installed after the grace period.

Related Documentation

- Junos OS Feature Licenses on page 287
- License Enforcement on page 287
- Software Feature Licenses on page 292
- Verifying Junos OS License Installation on page 316
- **show system license on page 430**

Software Feature Licenses

Each license is tied to one software feature pack, and that license is valid for only one device.

For information about how to purchase software licenses, contact your Juniper Networks sales representative at http://www.juniper.net/in/en/contact-us/.

- Software Features That Require Licenses on M Series, MX Series, and T Series Routers on page 292
- Software Features That Require Licenses on M Series Routers Only on page 295
- Software Features That Require Licenses on MX Series Routers Only on page 296
- Software Features That Require Licenses on J Series and SRX Series Devices on page 300
- Software Features That Require Licenses on EX Series Switches on page 308
- Software Features That Require Licenses on the QFX Series on page 310

Software Features That Require Licenses on M Series, MX Series, and T Series Routers

Table 30 on page 293 lists the licenses you can purchase for each M Series, MX Series, and T Series software feature. Each license allows you to run the specified software feature on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at http://www.juniper.net/in/en/contact-us/.

Table 30: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers

Licensed Software Feature	Supported Devices	Model Number
Generalized Multi-Protocol Label Switching (GMPLS) Support on Junos OS	M10i, M7i, M120, M160, M20, M320, M40e, T320, T640, and MX Series Routers	JS-GMPLS
IPv6 Support on Junos OS	M120, M160, M20, M320, M40e, T320, T640, and MX Series Routers	JS-IPv6
Logical Router Support for Junos OS	M10i, M120, M160, M20, M320, M40e, M7i, T320, T640, and MX Series Routers	JS-LR
J- Flow accounting license for Adaptive Services (AS) PIC and Multiservices PIC	M10i, M120, M160, M20, M320, M40e, M7i, T320, M10, M5, T640, and T1600	S-ACCT
Chassis license for Application Traffic Optimization service, policy enforcement and application statistics. This license includes S-AI and S-LDPF fucntionality, and 1 Year Signature Subscription License	MX104, MX240, MX480, MX960, M Series, and T Series Routers	S-ATO
Software License for Passive Monitoring Flow Collector Application, supporting 100Kpps throughput; Chassis based license for Multiservices PIC.	M320, T640, T320, T1600	S-COLLECTOR-100K
License to use Compressed Real-Time Transport Protocol (CRTP) feature in AS PIC and Multiservices PIC	M10i, M120, M160, M20, M320, M40e, M7i, T320, M10, M5, T640, and T1600	S-CRTP
Software License for Passive Monitoring DFC Application, supporting 100Kpps throughput; Chassis based license for Multiservices PIC	M320, T640, T320, T1600	S-DFC-100K
Security Services license for AS PIC and Multiservices PIC	M10i, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10, T1600	S-ES
Chassis license for IDP service, policy enforcement. This license includes S-AI and S-LDPF fucntionality, and 1 Year Signature Subscription License	MX104, MX240, MX480, MX960, M Series, and T Series Routers	S-IDP
Junos-FIPS Software License	M10i, M7i, M320, M40e, T320, T640	S-JUNOS-FIPS
Link Services Software License—up to 1023 ML bundles per Chassis for Multiservices PIC and Multiservices Dense Port Concentrator (DPC)	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960	S-LSSL-1023

Table 30: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Link Services Software Ugrade License—from 255 to 1023 ML bundles per Chassis for Multiservices PIC and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960	S-LSSL-1023-UPG
Link Services Software Ugrade License—from 64 to 255 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960	S-LSSL-255-UPG
Link Services Software License—up to 255 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M10, M7i, M5, M120, M20, M320, M40e, T320, T640, M10i, T1600, MX240, MX480, MX960	S-LSSL-256
Link Services Software License—up to 4 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M10i, M120, M20, M320, M40e, M7i, T320, M10, M5, T640, T1600, MX240, MX480, MX960	S-LSSL-4
Link Services Software License—up to 64 ML bundles per Chassis for AS PIC, MS PIC and MS DPC	M10, M7i, M5, M120, M20, M320, M40e, T320, T640, M10i, T1600, MX240, MX480, MX960	S-LSSL-64
Link Services Software Upgrade License—from 4 to 64 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960	S-LSSL-64-UPG
Software License for Passive Monitoring Flow Monitor Application, supporting 1M flows. Chassis based license for Multiservices PIC	M320, T640, T320, T1600	S-MONITOR-1M
Network Address Translation (NAT), FW license on AS PIC and Multiservices PIC: Multi-instance	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, T1600	S-NAT-FW-MULTI
NAT, FW license on AS PIC and Multiservices PIC: Single-instance	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, T1600	S-NAT-FW-SINGLE
Software license for Packet trigger subscriber policy	MX240, MX480, MX960, M120, M320	S-PTSP
Subscriber Access Feature Pack License Scaling (128000)	MX104, MX240, MX480, MX960, M120, M320	S-SA-128K
Subscriber Access Feature Pack License Scaling (32000)	MX104, MX240, MX480, MX960, M120, M320	S-SA-32K
Subscriber Access Feature Pack License Scaling (4000)	MX104, MX240, MX480, MX960, M120, M320, MX80	S-SA-4K
Subscriber Access Feature Pack License Scaling (64000)	MX104, MX240, MX480, MX960, M120, M320	S-SA-64K

Table 30: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Subscriber Access Feature Pack License Scaling (8000)	MX104, MX240, MX480, MX960, M120, M320, MX80	S-SA-8K
Subscriber Access Feature Pack License Scaling (96000)	MX104, MX240, MX480, MX960, M120, M320	S-SA-96K
Subscriber Access Feature Pack license	MX104, MX240, MX480, MX960, M120, M320	S-SA-FP
Stateful Failover for Services on AS PIC and Multiservices PIC: Multilink PPP (MLPPP) only	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, T1600	S-SERVICES-SFO
Subscriber Service Management Feature Packet License (RADIUS/SRC based Service Activation and Deactivation) Per-Service Accounting Features for Subscribers	MX104, MX240, MX480, MX960, M120, M320	S-SSM-FP
Subscriber Traffic Lawful Intercept Feature Pack License	MX240, MX480, MX960, M120, M320, MX80	S-SSP-FP
Software license for application aware traffic direct feature	MX240, MX480, MX960, M120, M320	S-TFDIRECT-APP
Software license for subscriber aware traffic direct feature	MX240, MX480, MX960, M120, M320	S-TFDIRECT-SUB
Video Services Feature Pack license	M120, M320, MX80, MX104, MX240, MX480, MX960	S-VIDEO-FP
Port capacity enhancement Feature Pack License for MX5 routers	MX5	mx5-to-mx10-upgrade
Port capacity enhancement Feature Pack License for MX10 routers	MX10	mx10-to-mx40-upgrade
Port capacity enhancement Feature Pack License for MX40 routers	MX40	mx40-to-mx80-upgrade

Software Features That Require Licenses on M Series Routers Only

Table 31 on page 296 lists the licenses you can purchase for each M Series software feature. Each license allows you to run the specified software feature on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at http://www.juniper.net/in/en/contact-us/.

Table 31: Junos OS Feature License Model Number for M Series Routers

Licensed Software Feature	Supported Devices	Model Number
J-Flow accounting license on Integrated Adaptive Services Module (ASM) and Integrated Multi-Services Module	M7i	S-ACCT-BB
Security Services license on ASM and Integrated Multi-Services Module	M7i	S-ES-BB
Layer 2 Tunneling Protocol (L2TP) L2TP Network Server (LNS) license for 16000 sessions on Multiservices PIC	M120	S-LNS-16K
L2TP LNS license Upgrade—from 8000 to 16000 sessions on Multiservices PIC	M120	S-LNS-16K-UPG
L2TP LNS license for 2000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, M120	S-LNS-2K
L2TP LNS license for 4000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, M120	S-LNS-4K
L2TP LNS license Upgrade—from 2000 to 4000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, M120	S-LNS-4K-UPG
L2TP LNS license for 8000 sessions on Multiservices PIC	M7i, M10i, M120	S-LNS-8K
L2TP LNS license Upgrade—from 4000 to 8000 sessions on AS PIC and Multiservices PIC	M7i, M10i, M120	S-LNS-8K-UPG
Link services software license on integrated ASM and Integrated Multi Services Module—up to 4 ML bundles	M7i	S-LSSL-BB
NAT, FW license on Integrated ASM and Integrated Multi Services Module: Multi instance	M7i	S-NAT-FW-MULTI-BB
NAT, FW license on Integrated ASM and Integrated Multi Services Module: Single instance	M7i	S-NAT-FW-SINGLE-BB
Tunnel services software license for AS PIC and Multiservices PIC (chassis license)	M7i, M10i	S-TUNNEL

Software Features That Require Licenses on MX Series Routers Only

Table 32 on page 297 lists the licenses you can purchase for each MX Series software feature. Each license allows you to run the specified software feature on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at http://www.juniper.net/in/en/contact-us/.

Table 32: Junos OS Feature License Model Number for MX Series Routers

Licensed Software Feature	Supported Devices	Model Number
Upgrade license—from MX80-10G-ADV to MX80-40G-ADV	MX80	MX80-10G40G-UPG-ADV-B
Upgrade license—from MX80-10G to MX80-40G	MX80	MX80-10G40G-UPG-B
Upgrade license—from MX80-40G-ADV to full MX80	MX80	MX80-40G-UPG-ADV-B
Upgrade license—from MX80-40G to full MX80	MX80	MX80-40G-UPG-B
Upgrade license-–from MX80-5G-ADV to MX80-10G-ADV	MX80	MX80-5G10G-UPG-ADV-B
Upgrade license—from MX80-5G to MX80-10G	MX80	MX80-5G10G-UPG-B
Upgrade license to activate 2x10GE P2&3	MX104	S-MX104-ADD-2X10GE
Upgrade license to activate 2X10GE P0&1	MX104	S-MX104-UPG-2X10GE
Upgrade license to activate 4X10GE fixed ports on MX104	MX104	S-MX104-UPG-4X10GE
License to support per VLAN queuing on MX104	MX104	S-MX104-Q
Chassis-based software license for inline J-Flow monitoring on MX5, MX10, M40, MX80, and MX104 Series routers	MX5, MX10, M40, MX80, and MX104	S-JFLOW-CH-MX5-104
Flow monitoring and accounting features using J-Flow service on any Modular Port Concentrator (MPC) or MS-DPC	MX240, MX480, MX960	S-ACCT-JFLOW-CHASSIS
Software License for in-line J-Flow service on Trio MPCs	MX240, MX480, MX960	S-ACCT-JFLOW-IN
Flow monitoring and accounting features using J-Flow service on any MPC limited to 10G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-10G
Flow monitoring and accounting features using J-Flow service on any MPC limited to 10G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-10G-UPG
Flow monitoring and accounting features using J-Flow service on any MPC limited to 5G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-5G
2000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-2K
4000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-4K
Upgrade from 2000 IKE sessions to 4000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-4K-UPG
6000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-6K

Table 32: Junos OS Feature License Model Number for MX Series Routers *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Upgrade from 4000 IKE sessions to 6000 IKE Sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-6K-UPG
License to support DS3 Channelization (down to DS0) on each Modular Interface Card (MIC) for MIC-3D-8DS3-E3; also requires license S-MX80-Q when used on the MX80 platform	MX80, MX104, MX240, MX480, MX960	S-MIC-3D-8CHDS3
License to support full-scale L3 routes and L3 VPN	MX80	S-MX80-ADV-R
License to support 256K routes	MX104	S-MX104-ADV-R1
License to support scaling L3 and VPN routes to 1 million or more entries on MX104 platforms	MX104	S-MX104-ADV-R2
License to support full-scale L3 routes and L3 VPN on each slot for MPC-3D-16XGE-SFPP	MX240, MX480, MX960	S-MPC-3D-16XGE-ADV-R
License to support full-scale L3 routes and L3 VPN on each slot for port queuing MPCs	MX240, MX480, MX960	S-MPC-3D-PQ-ADV-R
License to support full-scale L3 routes and L3 VPN on each slot for hierarchical quality of service (HQoS) MPCs	MX240, MX480, MX960	S-MPC-3D-VQ-ADV-R
Subscriber Management Feature Pack License for MX80	MX80	S-MX80-SA-FP
Subscriber Management Feature Pack for MX104 series	MX104	S-MX104-SA-FP
Subscriber Service Management Feature Packet License—RADIUS and SRC-based service activation and deactivation per-service accounting features	MX80	S-MX80-SSM-FP
Subscriber Service Management Feature Packet License	MX104	S-MX104-SSM-FP
Upgrade to Traffic Direct Advanced (per MS-DPC)	MX960	S-MX-TD-UPG
License to run one instance of the NAT software on one NPU per MS-DPC	MX240, MX480, MX960	S-NAT
License to support inline NAT software on MX5, MX10, MX40, MX80, MX104	MX5, MX10, MX40, MX80, MX104	S-NAT-IN-MX5-104 (Replaces S-NAT-IN-MX40-MX80 and S-NAT-IN-MX5-MX10)
License to run one instance of the NAT software on one NPU per MS-MIC, MS-DPC, or MS-MPC	MX80, MX104, MX240, MA480, MX960, MX2010, MX2020	S-NAT-NPU (Replaces S-NAT-IN-MX40-MX80-UPG)
License to run NAT using any MPC in an MX Chassis	MX240, MX480, MX960	S-NAT-IN-MX-CHASSIS
Subscriber Access Feature Pack License Scaling (4000)	MX240, MX480, MX960, M120, M320, MX80	S-SA-4K

Table 32: Junos OS Feature License Model Number for MX Series Routers *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Subscriber Access Feature Pack License Scaling (8000)	MX240, MX480, MX960, M120, M320, MX80	S-SA-8K
Subscriber Access Feature Pack License Scaling (16,000)	MX240, MX480, MX960, MX80	S-SA-16K
Subscriber Access Feature Pack License Scaling (32,000)	MX240, MX480, MX960, M120, M320	S-SA-32K
Subscriber Access Feature Pack License Scaling (64,000)	MX240, MX480, MX960, M120, M320	S-SA-64K
Subscriber Access Feature Pack License Scaling (96,000)	MX240, MX480, MX960, M120, M320	S-SA-96K
Subscriber Access Feature Pack License Scaling (128,000)	MX240, MX480, MX960, M120, M320	S-SA-128K
Subscriber Access Feature Pack License Scaling (256,000)	MX240, MX480, MX960	S-SA-256K
Subscriber Access Feature Pack License	MX240, MX480, MX960, M120, M320	S-SA-FP
Software License for Secure Flow Mirroring Service (FlowTap) (does not require MS-DPC)	MX80, MX104, MX240, MX480, MX960	S-SFM-FLOWTAP-IN
License to run one instance of the SFW and software on a MS-DPC	MX960, MX480, MX240	S-SFW
Subscriber Service Management Feature Packet License—RADIUS and SRC-based service activation and deactivation per-service accounting features	MX240, MX480, MX960, M120, M320	S-SSM-FP
Software license for one member of an MX Virtual Chassis	MX960, MX480, MX240	S-VCR
Upgrade license—from MX10 to equivalent of MX40; allows additional 2x10G fixed ports to be used on the MX10 router	MX10-T	MX10-40-UPG
Upgrade license—from MX10 to equivalent of MX80; allows additional 4x10G fixed ports to be used on the MX10 router	MX10-T	MX10-80-UPG
Upgrade license—from MX40 to equivalent of MX80; allows additional 2x10G fixed ports to be used on the MX40 router	MX40-T	MX40-80-UPG
Upgrade license—from MX5 to equivalent of MX10; allows second MIC slot to be used on the MX5 router	MX5-T	MX5-10-UPG
Upgrade license—from MX5 to equivalent of MX40; allows second MIC slot and 2x10G fixed ports to be used on the MX5 router	MX5-T	MX5-40-UPG

Table 32: Junos OS Feature License Model Number for MX Series Routers *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Upgrade license—from MX5 to equivalent of MX80. Allows second MIC slot and 4x10G fixed ports to be used on the MX5 router	MX5-T	MX5-80-UPG
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 4000 through 8000 subscribers	MX80, MX960, MX480, MX240	S-SA-UP-8K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 8000 through 16,000 subscribers	MX80, MX960, MX480, MX240	S-SA-UP-16K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 16,000 through 32,000 subscribers	MX240, MX480, MX960	S-SA-UP-32K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 32,000 through 64,000 subscribers	MX240, MX480, MX960	S-SA-UP-64K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 64,000 through 96,000 subscribers	MX240, MX480, MX960	S-SA-UP-96K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 96,000 through 128,000 subscribers	MX240, MX480, MX960	S-SA-UP-128K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 128,000 through 256,000 subscribers	MX240, MX480, MX960	S-SA-UP-256K

Software Features That Require Licenses on J Series and SRX Series Devices

For information about how to purchase a software license, contact your Juniper Networks sales representative at http://www.juniper.net/in/en/contact-us/.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. Table 33 on page 300 describes the Junos OS features that require licenses.

Table 33: Junos OS Feature Licenses

Junos OS License Requirements	Device										
Feature	J Series	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650	SRX1400	SRX3000 line	SRX5000 line
Access Manager		X	X	X	X	X	X	X			
BGP Route Reflectors	X							X			
Dynamic VPN		X	X	X	X	X	X	X			

Table 33: Junos OS Feature Licenses *(continued)*

Junos OS License Requirements	Device										
Feature	J Series	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650	SRX1400	SRX3000 line	SRX5000 line
IDP Signature Update	X	X *	X	X *	X *	X *	X	X	X	X	X
Application Signature Update (Application Identification)	X	X	X	X	X	X	X	X	X	X	X
J-Flow License (For Junos Release 9.5 and earlier)	X										
Juniper-Kaspersky Antivirus	X	X	X	X	X	X	X	X			
Juniper-Sophos Antispam	X	X	X	X	X	X	X	X			
Juniper-Websense Web filtering	X	X	X	X	X	X	X	X			
Logical Systems									X	X	X
SRX100 Memory Upgrade		X									
UTM	X	X*	X	X *	X	X *	X	X			

* Indicates support on high-memory devices only.

Table 34 on page 301 lists the licenses you can purchase for each J Series or SRX Series software feature. Each license allows you to run the specified advanced software features on a single device.

Table 34: Junos OS Feature License Model Number for J Series and SRX Series Devices

Licensed Software Feature	Supported Devices	Model Number
Memory Software License (Upgrades SRX100B model from 512-MB RAM to 1-GB RAM)	SRX100	SRX100-MEM-LIC-UPG
Advanced BGP License	J4350, J6350, J2320, J2350	JX-BGP-ADV-LTU
	SRX650 only	SRX-BGP-ADV-LTU

Table 34: Junos OS Feature License Model Number for J Series and SRX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Application Security and IPS updates (1 year, 3 years, and 5 years)	SRX100	SRX100-APPSEC-A-1 SRX100-APPSEC-A-3 SRX100-APPSEC-A-5
	SRX210, SRX220, and SRX240	SRX2XX-APPSEC-A-1 SRX2XX-APPSEC-A-3 SRX2XX-APPSEC-A-5
	SRX550	SRX550-APPSEC-A-1 SRX550-APPSEC-A-3 SRX550-APPSEC-A-5
	SRX650	SRX650-APPSEC-A-1 SRX650-APPSEC-A-3 SRX650-APPSEC-A-5
	SRX1400	SRX1400-APPSEC-A-1 SRX1400-APPSEC-A-3 SRX1400-APPSEC-A-1-R SRX1400-APPSEC-A-3-R
	SRX3400	SRX3400-APPSEC-A-1 SRX3400-APPSEC-A-3
	SRX3600	SRX3600-APPSEC-A-1 SRX3600-APPSEC-A-3
	SRX5600	SRX5600-APPSEC-A-1 SRX5600-APPSEC-A-3
	SRX5800	SRX5800-APPSEC-A-1 SRX5800-APPSEC-A-3

Table 34: Junos OS Feature License Model Number for J Series and SRX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
IDP updates (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-IDP SRX1XX-IDP-3 SRX1XX-IDP-5
	SRX210, SRX220, SRX240	SRX2XX-IDP SRX2XX-IDP-3 SRX2XX-IDP-5
	SRX550	SRX550-IDP SRX550-IDP-3 SRX550-IDP-5
	SRX650	SRX650-IDP SRX650-IDP-3 SRX650-IDP-5
IPS subscription (1 year and 3 years)	SRX3400, SRX3600	SRX3K-IDP SRX3K-IDP-3
	SRX5600, SRX5800	SRX5K-IDP SRX5K-IDP-3 SRX5K-IDP-3-R SRX5K-IDP-R

Table 34: Junos OS Feature License Model Number for J Series and SRX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Juniper-Kaspersky Antivirus updates (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-K-AV SRX1XX-K-AV-3 SRX1XX-K-AV-5
	SRX210, SRX220, SRX240	SRX2XX-K-AV SRX2XX-K-AV-3 SRX2XX-K-AV-5
	SRX550	SRX550-K-AV SRX550-K-AV-3 SRX550-K-AV-5
	SRX650	SRX650-K-AV SRX650-K-AV-3 SRX650-K-AV-5
Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-S-AV SRX1XX-S-AV-3 SRX1XX-S-AV-5
	SRX210, SRX220, SRX240	SRX2XX-S-AV SRX2XX-S-AV-3 SRX2XX-S-AV-5
	SRX550	SRX550-S-AV SRX550-S-AV-3 SRX550-S-AV-5
	SRX650	SRX650-S-AV SRX650-S-AV-3 SRX650-S-AV-5

Table 34: Junos OS Feature License Model Number for J Series and SRX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-S2-AS SRX1XX-S2-AS-3 SRX1XX-S2-AS-5
	SRX210, SRX220, SRX240	SRX2XX-S2-AS SRX2XX-S2-AS-3 SRX2XX-S2-AS-5
	SRX550	SRX550-S2-AS SRX550-S2-AS-3 SRX550-S2-AS-5
	SRX650	SRX650-S2-AS SRX650-S2-AS-3 SRX650-S2-AS-5
Juniper-Websense Web filtering (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-W-EWF SRX1XX-W-EWF-3 SRX1XX-W-EWF-5
	SRX210, SRX220, SRX240	SRX2XX-W-WF SRX2XX-W-WF-3 SRX2XX-W-WF-5
	SRX550	SRX550-W-WF SRX550-W-WF-3 SRX550-W-WF-5
	SRX650	SRX650-W-WF SRX5650-W-WF-3 SRX650-W-WF-5

Table 34: Junos OS Feature License Model Number for J Series and SRX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Enterprise—Kaspersky Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-SMB4-CS SRX1XX-SMB4-CS-3 SRX1XX-SMB4-CS-5
	SRX210, SRX220, SRX240	SRX2XX-SMB4-CS SRX2XX-SMB4-CS-3 SRX2XX-SMB4-CS-5
	SRX550	SRX550-SMB4-CS SRX550-SMB4-CS-3 SRX550-SMB4-CS-5
	SRX650	SRX650-SMB4-CS SRX650-SMB4-CS-3 SRX650-SMB4-CS-5
Enterprise—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-S-SMB4-CS SRX1XX-S-SMB4-CS-3 SRX1XX-S-SMB4-CS-5
	SRX210, SRX220, SRX240	SRX2XX-S-SMB4- CS SRX2XX-S-SMB4- CS-3 SRX2XX-S-SMB4- CS-5
	SRX550	SRX550-S-SMB4- CS SRX550-S-SMB4- CS-3 SRX550-S-SMB4- CS-5
	SRX650	SRX650-S-SMB4- CS SRX650-S-SMB4- CS-3 SRX650-S-SMB4- CS-5
Dynamic VPN Client (5, 10, and 25 simultaneous users)	SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650	SRX-RAC-5-LTU SRX-RAC-10-LTU SRX-RAC-25-LTU

Table 34: Junos OS Feature License Model Number for J Series and SRX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Dynamic VPN Service (5, 10, 25, and 50 simultaneous users)	SRX210, SRX240, SRX100, SRX220, SRX650, SRX110, SRX550	SRX-RAC-5-LTU
	SRX210, SRX240, SRX100, SRX220, SRX650, SRX110, SRX550	SRX-RAC-10-LTU
	SRX210, SRX240, SRX100, SRX220, SRX650, SRX550	SRX-RAC-25-LTU
	SRX240, SRX650, SRX220, SRX210, SRX550	SRX-RAC-50-LTU
Dynamic VPN Service (100 and 150 simultaneous users)	SRX650, SRX220, SRX240, SRX550	SRX-RAC-100-LTU
		SRX-RAC-150-LTU
Dynamic VPN Service (250 simultaneous users)	SRX650, SRX240, SRX550 NOTE: Requires Junos OS 11.2R3 or later	SRX-RAC-250-LTU
Dynamic VPN Service (500 simultaneous users)	SRX650, SRX550 NOTE: Requires Junos OS 11.2R3 or later	SRX-RAC-500-LTU
J-Flow License (For Junos Release 9.5 and earlier)	J4350, J6350, J2320, J2350	JX-JFlow-LTU
Services Offload License	SRX1400	SRX1K-SVCS-OFFLOAD-RTU
	SRX3400, SRX3600	SRX3K-SVCS-OFFLOAD-RTU
	SRX5600, SRX5800	SRX5K-SVCS-OFFLOAD-RTU

Table 34: Junos OS Feature License Model Number for J Series and SRX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Logical Systems License (incremental 1, 5, and 25 numbers)	SRX1400	SRX-1400-LSYS-1
		SRX-1400-LSYS-25
		SRX-1400-LSYS-5
	SRX3400	SRX-3400-LSYS-1
		SRX-3400-LSYS-5
		SRX-3400-LSYS-25
	SRX3600	SRX-3600-LSYS-1
		SRX-3600-LSYS-5
		SRX-3600-LSYS-25
	SRX5600	SRX-5600-LSYS-1
		SRX-5600-LSYS-5
		SRX-5600-LSYS-25
	SRX5800	SRX-5800-LSYS-1
		SRX-5800-LSYS-5
		SRX-5800-LSYS-25

Software Features That Require Licenses on EX Series Switches

The following Junos OS features require an Enhanced Feature License (EFL) or Advanced Feature License (AFL) on EX Series devices:

- (EX2200 only) Bidirectional forwarding detection (BFD)
- (EX2200 only) Connectivity fault management (IEEE 802.lag)
- (EX2200 only) Internet Group Management Protocol version 1 (IGMPv1), IGMPv2, and IGMPv3
- (EX2200 and EX3300) OSPFv1/v2 (with 4 active interfaces)
- (EX2200 only) Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- (EX2200 and EX3300) Q-in-Q tunneling (IEEE 802.lad)

- (EX2200 only) Real-time performance monitoring (RPM)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) Intermediate System-to-Intermediate System (IS-IS)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) IPv6 protocols: OSPFv3, PIPng, IS-IS for IPv6, IPv6 BGP
- (EX3200, EX4200, EX4500, EX6200, and EX8200) MPLS with RSVP-based label-switched paths (LSPs) and MPLS-based circuit cross-connects (CCCs)

Table 35 on page 309 lists the licenses you can purchase for each EX Series software feature. Each license allows you to run the specified enhanced software features on a single device.

NOTE:

For a Virtual Chassis deployment, two license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role:

- In an EX8200 Virtual Chassis, the devices in the master and backup roles are always XRE200 External Routing Engines.
- In all other Virtual Chassis, the devices in the master and backup roles are switches.

You do not need additional license keys for Virtual Chassis member switches that are in the licensed role or for the redundant Routing Engine (RE) modules or the redundant Switch Fabric and Routing Engine (SRE) modules in an EX8200 member switch.

For more details regarding EX Series feature licenses, see *Understanding Software Licenses for EX Series Switches*.

For information about how to purchase a software license, contact your Juniper Networks sales representative at http://www.juniper.net/in/en/contact-us/.

Table 35: Junos OS Enhanced Feature License (EFL) and Advanced Feature License (AFL) Model Number for EX Series Devices

Licensed Software Feature	Supported Devices	Model Number
Enhanced Feature License for EX 2200-24T/P	EX2200	EX-24-EFL
Enhanced Feature License for EX 2200-48T/P	EX2200	EX-48-EFL
Enhanced Feature License for EX2200-C	EX2200-C	EX-12-EFL

Table 35: Junos OS Enhanced Feature License (EFL) and Advanced Feature License (AFL) Model Number for EX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Advanced Feature License for EX 3200-24T/P and EX 4200-24T/P/F/PX	EX3200, EX4200	EX-24-AFL
Advanced Feature License for EX 3200-48T/P, EX 4200-48T/P/F/PX, and EX4500-40F	EX3200, EX4200, EX4500	EX-48-AFL
Advanced Feature License for EX6200	EX6200	EX6200-AFL
XRE200 Advanced Feature License for EX8200	EX8200	EX-XRE200-AFL
Advanced Feature License for EX8208	EX8208	EX8208-AFL
Advanced Feature License for EX8216	EX8216	EX8216-AFL

Software Features That Require Licenses on the QFX Series

NOTE: If you try to configure a feature that is not licensed, you will receive syslog messages saying that you are using a feature that is licensable and that you do not possess a license for the feature. If you try to commit configuration changes for a feature that is not licensed, you will receive a commit warning saying that you have exceeded the allowed license limit for the feature.

NOTE: There is no separate license for Virtual Chassis like there is for Virtual Chassis Fabric.

Table 36 on page 311 lists the licenses you can purchase for each QFX Series software feature.

For information about how to purchase a software license, contact your Juniper Networks sales representative.

Table 36: Junos OS Feature Licenses and Model Numbers for QFX Series Devices

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX3500, QFX3600, QFX5100-48S, and QFX5100-48T switches	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX-JSL-EDGE-ADV1
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN) and Open vSwitch Database (OVSDB)	QFX5100-24Q and QFX5100-96S switches	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX5100-HDNSE-LIC
QFX Series advanced feature license for Border Gateway Protocol (BGP)	QFX3100 Director device	One per Node device in a network Node group	QFX-JSL-DRCTR-ADV1
QFX Series advanced feature license for Fibre Channel	QFX3500 switch	One per switch on which fibre channel ports are configured	QFX-JSL-EDGE-FC
QFX Series advanced feature license for Fibre Channel	QFX3100 Director device	One per QFX3500 Node device on which fibre channel ports are configured	QFX-JSL-DRCTR-FC
QFX Series advanced feature license for Fibre Channel - Capacity 16	QFX3100 Director device	One for up to 16 QFX3500 Node devices on which fibre channel ports are configured	QFX-JSL-DRCTR-FC-C16
QFX Series feature license for enabling fabric mode	QFX3500 and QFX3600 device	One per device	QFX3000-JSL-EDGE-FAB
QFX Series feature license for base software for QFX3000-G QFabric system	QFX3100 Director device	One per QFX3000-G QFabric system	QFX3008-JSL-DRCTR-FAB
QFX Series feature license for base software for QFX3000-M QFabric system	QFX3100 Director device	One per QFX3000-M QFabric system	QFX3000M-JSL-DRCTR-FAB

Table 36: Junos OS Feature Licenses and Model Numbers for QFX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX and EX Series feature license for enabling Media Access Control security (MACsec)	QFX switches that support MACsec. See *Understanding Media Access Control Security (MACsec)*.	One per switch, two per Virtual Chassis,	EX-QFX-MACSEC-AGG
Virtual Chassis Fabric (VCF)	All member devices in a Virtual Chassis Fabric (VCF)	Two per Virtual Chassis Fabric (VCF)	QFX-VCF-LIC

CHAPTER 15

Installing and Managing Licenses

Adding New Licenses (CLI Procedure)

Before adding new licenses, complete the following tasks:

- Purchase the required licenses.
- Establish basic network connectivity with the router or switch. For instructions on establishing basic connectivity, see the *Getting Started Guide* or *Quick Start Guide* for your device.

NOTE: **On QFabric systems, install your licenses in the default partition of the QFabric system and not on the individual components (Node devices and Interconnect devices).**

To add a new license key to the device using the CLI:

1. From the CLI operational mode, enter one of the following CLI commands:
   - To add a license key from a file or URL, enter the following command, specifying the filename or the URL where the key is located:

     user@host> **request system license add *filename* | *url***
   - To add a license key from the terminal, enter the following command:

     user@host> **request system license add terminal**
2. When prompted, enter the license key, separating multiple license keys with a blank line.

   If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit license entry mode.
3. Go on to "Verifying Junos OS License Installation" on page 316.

On routers that have graceful Routing Engine switchover (GRES) enabled, after successfully adding the new license on the master Routing Engine, the license keys are automatically synchronized on the backup Routing Engine as well. However, in case GRES is not enabled, the new license is added on each Routing Engine separately. This ensures that the license key is enabled on the backup Routing Engine during changeover of mastership between the Routing Engines.

To add a new license key to a router with dual Routing Engines without GRES:

1. After adding the new license key on the master Routing Engine, use the **request chassis routing-engine master switch** command to have the backup Routing Engine become the master Routing Engine.
2. Log in to the active Routing Engine and add the new license key, repeat the same step.

NOTE: **Adding a license key to the router or switch might be delayed if a kernel resynchronization operation is in progress at that time. The following message is displayed on the CLI when the license-adding operation is about to be delayed:**
A kernel re-sync operation is in progress. License update may take several minutes to complete.

Related Documentation

- Deleting a License (CLI Procedure) on page 314
- Junos OS Feature Licenses on page 287
- Verifying Junos OS License Installation on page 316
- **request system license add on page 350**

Deleting a License (CLI Procedure)

Before deleting a license, establish basic network connectivity with the router or switch. For instructions on establishing basic connectivity, see the *Getting Started Guide* or *Quick Start Guide* for your router or switch.

You have the options to delete a single license, delete all licenses, or delete a list of licenses enclosed in brackets.

1. Display the licenses available to be deleted.

```
user@host> request system license delete license-identifier-list ?
Possible completions:
  E00468XXX4           License key identifier
  JUNOS10XXX1          License key identifier
  JUNOS10XXX2          License key identifier
  JUNOS10XXX3          License key identifier
  JUNOS10XXX4          License key identifier
  [                    Open a set of values
```

2. To delete a license key or keys from a device using the CLI operational mode, select one of the following methods:

- Delete a single license by specifying the license ID. Using this option, you can delete only one license at a time.

  user@host> **request system license delete** ***license-identifier***

- Delete all license keys from the current device.

  user@host> **request system license delete all**

- Delete multiple license keys from the current device. Specify the license identifier for each key and enclose the list of identifiers in brackets.

  user@host> **request system license delete license-identifier-list [*JUNOS10XXX1 JUNOS10XXX3 JUNOS10XXX4 ...*]**

```
Delete license(s) ?
 [yes,no] (no) yes
```

3. Go on to "Verifying Junos OS License Installation" on page 316.

NOTE: Deleting a license key from the router or switch might be delayed if a kernel resynchronization operation is in progress at that time. The following message is displayed on the CLI when the license-deleting operation is about to be delayed:
A kernel re-sync operation is in progress. License update may take several minutes to complete.

Related Documentation

- Adding New Licenses (CLI Procedure) on page 313
- Saving License Keys on page 315
- Junos OS Feature Licenses on page 287
- Verifying Junos OS License Installation on page 316
- **request system license delete on page 351**

Saving License Keys

Before saving a license, establish basic network connectivity with the router or switch. For instructions on establishing basic connectivity, see the *Getting Started Guide* or *Quick Start Guide* for your router or switch.

To save the licenses installed on a device to a file using the CLI:

1. From the CLI operational mode, enter one of the following CLI commands:

   - To save the installed license keys to a file or URL, enter the following command:

     user@host> **request system license save** ***filename | url***

     For example, the following command saves the installed license keys to a file named **license.config**:

   - To save a license key from the terminal, enter the following command:

```
user@host> request system license save ftp://user@host/license.config
```

2. Go on to "Verifying Junos OS License Installation" on page 316.

Related Documentation

- Adding New Licenses (CLI Procedure) on page 313
- Deleting a License (CLI Procedure) on page 314
- Junos OS Feature Licenses on page 287
- Verifying Junos OS License Installation on page 316

Verifying Junos OS License Installation

To verify Junos OS license management, perform the following tasks:

- Displaying Installed Licenses on page 316
- Displaying License Usage on page 317

Displaying Installed Licenses

Purpose Verify that the expected licenses are installed and active on the router or switch.

Action From the CLI, enter the **show system license** command.

Sample Output

```
user@host> show system license
License usage:
                    Licenses     Licenses    Licenses    Expiry
  Feature name         used    installed      needed
  subscriber-acct         0            1           0    permanent
  subscriber-auth         0            1           0    permanent
  subscriber-addr         0            1           0    permanent
  subscriber-vlan         0            1           0    permanent
  subscriber-ip           0            1           0    permanent
  scale-subscriber        0         1000           0    permanent
  scale-l2tp              0         1000           0    permanent
  scale-mobile-ip         0         1000           0    permanent

Licenses installed:
  License identifier: E000185416
  License version: 2
  Features:
    subscriber-acct  - Per Subscriber Radius Accounting
      permanent
    subscriber-auth  - Per Subscriber Radius Authentication
      permanent
    subscriber-addr  - Address Pool Assignment
      permanent
    subscriber-vlan  - Dynamic Auto-sensed Vlan
      permanent
    subscriber-ip    - Dynamic and Static IP
      permanent
```

Meaning The output shows a list of the license usage and a list of the licenses installed on the router or switch. Verify the following information:

- Each license is present. Licenses are listed in ascending alphanumeric order by license ID.
- The state of each license is **permanent**.

NOTE: **A state of invalid indicates that the license key is not a valid license key. Either it was entered incorrectly or it is not valid for the specific device.**

- The feature for each license is the expected feature. The features enabled are listed by license. An all-inclusive license has all features listed.
- All configured features have the required licenses installed. The Licenses needed column must show that no licenses are required.

Displaying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the router or switch.

Action From the CLI, enter the **show system license usage** command.

Sample Output

```
user@host> show system license usage
            Licenses     Licenses    Licenses    Expiry
  Feature name         used    installed      needed
  subscriber-addr         1            0           1    29 days
  scale-subscriber        0         1000           0    permanent
  scale-l2tp              0         1000           0    permanent
  scale-mobile-ip         0         1000           0    permanent
```

Meaning The output shows any licenses installed on the router or switch and how they are used. Verify the following information:

- Any configured licenses appear in the output. The output lists features in ascending alphabetical order by license name. The number of licenses appears in the third column. Verify that you have installed the appropriate number of licenses.
- The number of licenses used matches the number of configured features. If a licensed feature is configured, the feature is considered used. The sample output shows that the subscriber address pooling feature is configured.
- A license is installed on the router or switch for each configured feature. For every feature configured that does not have a license, one license is needed.

  For example, the sample output shows that the subscriber address feature is configured but that the license for the feature has not yet been installed. The license must be installed within the remaining grace period to be in compliance.

PART 4

Troubleshooting Information

CHAPTER 16

Troubleshooting Software Installation

Troubleshooting Software Installation

This topic describes troubleshooting issues with software installations on EX Series switches.

Recovering from a Failed Software Upgrade on an EX Series Switch

Problem **Description:** If Junos OS loads but the CLI is not working, or if the switch has no software installed, use this recovery installation procedure to install Junos OS.

Solution If there is already a Junos OS image on the system, you can either install the new Junos OS package in a separate partition and have both Junos OS images remain on the system, or you can wipe the disk clean before the new installation proceeds.

If there is no Junos OS image on the system, follow the instructions in "Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive" on page 210 to get an image on the system and boot the switch.

To perform a recovery installation:

1. Power on the switch. The loader script starts.

   After the message **Loading /boot/defaults/loader.conf** displays, you are prompted with:

   Hit [Enter] to boot immediately, or space bar for command prompt.

2. Press the space bar to enter the manual loader. The **loader>** prompt displays.

3. Enter the following command:

   loader> **install [– –format] [– –external]** ***source***

   where:

   - **format**—Use this option to wipe the installation media before installing the software package. If you do not include this option, the system installs the new Junos OS package in a different partition from the partition used by the most recently installed Junos OS package.
   - **external**—Use this option to install the software package on an external medium.
   - ***source***—Represents the name and location of the Junos OS package either on a server on the network or as a file on the USB flash drive:
     - Network address of the server and the path on the server; for example, **tftp://192.17.1.28/junos/jinstall-ex-4200-9.4R1.5-domestic-signed.tgz**
     - The Junos OS package on a USB device is commonly stored in the root drive as the only file; for example, **file:///jinstall-ex-4200-9.4R1.5-domestic-signed.tgz**

   The boot process proceeds as normal and ends with a login prompt.

Rebooting from the Inactive Partition

Problem **Description:** EX Series switches shipped with Junos OS Release 10.4R2 or earlier have Junos OS loaded on the system disk in partition 1. The first time you upgrade, the new software package is installed in partition 2. When you finish the installation and reboot, partition 2 becomes the active partition. Similarly, subsequent software packages are installed in the inactive partition, which becomes the active partition when you reboot at the end of the installation process.

On switches shipped with Release 10.4R3 and later, the same Junos OS image is loaded in each of the two root partitions, and you should copy the new software image to the alternate partition each time you upgrade.

If you performed an upgrade and rebooted, the system resets the active partition. You can use this procedure to manually boot from the inactive partition.

NOTE: **If you have completed the installation of the software image but have not yet rebooted, issue the request system software rollback command to return to the original software installation package.**

Solution Reboot from the inactive partition:

user@switch> **request system reboot slice alternate**

NOTE: If you cannot access the CLI, you can reboot from the inactive partition using the following procedure from the loader script prompt:

1. Unload and clear the interrupted boot from the active partition:

   loader> **unload**
   loader> **unset vfs.root.mountfrom**

2. Select the new (inactive) partition to boot from:

   loader> **set currdev=disk*x*s*y*:**

   where *x* is either 0 (internal) or 1 (external) and the y indicates the number of the inactive partition, either 1 or 2.

   You must include the colon (:) at the end of this command.

3. Boot Junos OS from the inactive partition:

   loader> **boot**

Freeing Disk Space for Software Installation

Problem **Description:** The software installation process requires a certain amount of unused disk space. If there is not enough space, you might receive an error message such as:

```
fetch: /var/tmp/incoming-package.tgz: No space left on device
```

Solution Identify and delete unnecessary files by using the **request system storage cleanup** command.

Installation from the Boot Loader Generates 'cannot open package' Error

Problem **Description:** When installing a Junos OS software image from the loader prompt, a "cannot open package error" is generated:

```
loader> install - -format
tftp://10.204.33.248/images/Flash_corr/official/jinstall-ex-4200-10.4I2011012-domestic-signed.tgz
Speed: 1000, full duplex
bootp: no reply
No response for RARP request
net_open: RARP failed
cannot open package (error 5)
```

Solution This might be due to the IP address, gateway IP address, netmask address, or server IP address not being properly set. You can set these values either from the shell or from the u-boot prompt.

To set these values from the shell:

% **nvram setenv ipaddr 10.204.35.235**
% **nvram setenv netmask 255.255.240.0**

```
% nvram setenv gatewayip 10.204.47.254
% nvram setenv serverip 10.204.33.248
```

To set these values from the u-boot prompt, log in to a console connection, reboot, and stop at the u-boot prompt (Cntrl+c):

```
=> setenv ipaddr 10.204.35.235
=> setenv gatewayip 10.204.47.254
=> setenv serverip 10.204.33.248
=> setenv netmask 255.255.240.0
=> saveenv
=> printenv Verify whether variables are set properly or not
=> boot
```

Related Documentation

- Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure) on page 52
- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) on page 132
- Installing Software on EX Series Switches (J-Web Procedure) on page 64
- Understanding Software Installation on EX Series Switches on page 35
- **show system storage partitions (EX Series Switches Only) on page 446**

Troubleshooting a Switch That Has Booted from the Backup Junos OS Image

Problem

Description: The switch boots from the backup root file partition. It is possible that the primary copy of JUNOS OS failed to boot properly, which could indicate that it is corrupted. This event is flagged in two ways:

- Upon login through the console or management port, the following warning message is displayed:

```
WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE

It is possible that the primary copy of JUNOS failed to boot up
properly, and so this device has booted from the backup copy.

Please re-install JUNOS to recover the primary copy in case
it has been corrupted.
```

- The following alarm message is generated:

```
user@switch> show chassis alarms
1 alarms currently active
Alarm time              Class  Description
2011-02-17 05:48:49 PST  Minor  Host 0 Boot from backup root
```

  If the switch is in a Virtual Chassis, the switch member number appears in the **Description** field, where the switch is called a host.

Solution

Install a new Junos OS image on the partition that had the corruption, or take a snapshot (use **request system snapshot**) of the currently active partition and use it to replace the image in the alternate partition:

If the switch is a standalone switch or a Virtual Chassis master switch, enter this command:

`user@switch>` **request system snapshot slice alternate**

If the switch is a Virtual Chassis member switch (not the master), enter this command on the Virtual Chassis:

`user@switch>` **request system snapshot slice alternate member** ***member-id***

where *member-id* is the Virtual Chassis member ID number.

Related Documentation

- Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 180
- Troubleshooting Software Installation on page 321
- **show system storage partitions (EX Series Switches Only) on page 446**

Disk Space Management for Junos OS Installation

A Junos OS installation or upgrade may fail if your router has a shortage of disk space. If a disk space error occurs, use one or more of the following options to complete the installation:

- Use the **request system storage cleanup** command to delete unnecessary files and increase storage space on the router.
- Specify the **unlink** option when you use the **request system software add** command to install the Junos OS:
  - On the J Series routers, the **unlink** option removes the software package at the earliest opportunity to create enough disk space for the installation to finish.
  - On the M Series, MX Series, and T Series routers, the **unlink** option removes the software package after a successful upgrade.
- Download the software packages you need from the Juniper Networks Support Web site, **http://www.juniper.net/support/**. The download program provides intelligent disk space management to enable installation.

NOTE: **If you are upgrading the J Series router from a remote location, the installation program automatically checks for enough disk space for the process to finish.**

Related Documentation

- *Junos OS Configuration Using the CLI*

Verifying PIC Combinations

On Juniper Networks routing platforms, you can typically install any combination of Physical Interface Cards (PICs) on a single Enhanced Flexible PIC Concentrator (FPC) or in two PIC slots served by a single Layer 2/Layer 3 Packet Processing application-specific integrated circuit (ASIC).

Newer Junos OS services for some PICs can require significant Internet Processor ASIC memory, and some configuration rules limit certain combinations of PICs if they are installed on some platforms.

During software installation, the configuration checker in the installation program checks the router's PICs. If any configuration rules affect your PIC combinations, the installation process stops and displays a message similar to the following:

```
The combination of PICS in FPC slot 3 is not supported with this release
    PIC slot 0 -
    PIC slot 1 - 1x OC-12 ATM-II IQ
    PIC slot 2 - 1x G/E IQ, 1000 BASE
    PIC slot 3 - 1x Link Service (4)
If you continue the installation, one or more PICs on
FPC slot 3 might appear to be online but
cannot be enabled and cannot pass traffic with this release of JUNOS.
See the Release Notes for more information.
WARNING: This installation attempt will be aborted. If you
WARNING: wish to force the installation despite these warnings
WARNING: you may use the 'force' option on the command line.
pkg_add: package /var/tmp/jbundle-7.6R1.x-domestic-signed.tgz fails requirements
 - not installed
```

The configuration checker has the following limitations:

- If a PIC is offline when you upgrade the router with new software, the configuration checker cannot detect PIC combinations affected by configuration rules and cannot warn about them.
- If you specify the **force** option when you upgrade the Junos OS, the configuration checker warns about the affected PIC combination and the software installation continues. However, after rebooting, one or more PICs might fail to initialize.
- The configuration checker looks for combinations of three affected PICs. If an Enhanced FPC contains four affected PICs, the script generates multiple warnings.

If you install a PIC into a router already running Junos OS, you can identify the presence of affected PIC combinations from messages in the system logging (**syslog**) file:

```
 Feb 6 17:57:40 CE1 feb BCHIP 0: uCode overflow - needs 129 inst space to load
b3_atm2_LSI_decode for stream 12
 Feb 6 17:57:41 CE1 chassisd[2314]: CHASSISD_IFDEV_DETACH_PIC:
ifdev_detach_pic(0/3)
 Feb 6 17:57:41 CE1 feb BCHIP 0: binding b3_atm2_LSI_decode to stream 12 failed
 Feb 6 17:57:41 CE1 feb PFE: can not bind B3 ucode prog b3_atm2_LSI_decode to FPC
 0: stream 12
```

For more information about checking for unsupported PIC combinations, see the corresponding PIC guide for your router, the *Junos OS Release Notes*, and *Technical Support Bulletin PSN-2004-12-002, PIC Combination Notes Summary* on the Juniper Networks Support Web site at **http://www.juniper.net/support/**.

For SRX Series Services Gateways

SRX5600 and SRX5800 devices support IOC or SPC on any given card slot, and there is no complexity in equipping the services gateways with the perfect balance of processing and I/O capacity. You can install upto 11 (on SRX5800) and five (SRX5600) SPCs and

IOCs on the device. However you must install atleast one SPC on device. For more details, see SRX5600 and SRX5800 Services Gateway Card Guide. SRX3600 supports a maximum of up to seven SPCs,three NPCs, six IOCs, and 11 NP-IOCs per chassis. However you must install at least one SPcs and NPC on the chassis. SRX3400 supports a maximum of up to four SPCs,two NPCs, four IOCs, and six NP-IOCs per chassis. However you must install at least one SPcs and NPC on the chassis. On SRX3400 and SRX3600 devices you must install PICs on the front slots of the chassis. For more details, see SR X1400 , SRX3400 , and SRX3600 Services Gateway Module Guide.

PART 5

Configuration Statements and Operational Commands

CHAPTER 17

Configuration Statements

auto-image-upgrade

Syntax auto-image-upgrade;

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 9.6 for EX Series switches.

Description Enable automatic software download on an EX Series switch acting as a DHCP client.

The DHCP client EX Series switch compares the software package name in the DHCP server message to the name of the software package that booted the switch. If the software packages are different, the DHCP client EX Series switch downloads and installs the software package specified in the DHCP server message.

Before you upgrade software using automatic software download, ensure that you have configured DHCP services for the switch, including configuring a path to a boot server and a boot file. See the *Junos OS System Basics Configuration Guide* for information about using the CLI to configure DHCP services and settings. See *Configuring DHCP Services (J-Web Procedure)* for information about using the J-Web interface to configure DHCP services and settings.

Default Automatic software download is disabled.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Upgrading Software by Using Automatic Software Download on page 178
- Understanding Software Installation on EX Series Switches on page 35
- *Understanding DHCP Services for Switches*

auto-snapshot

Syntax auto-snapshot;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description Enable the automatic snapshot feature, which allows the switch to automatically fix a corrupt Junos OS file in the primary root partition. If the automatic snapshot feature is enabled, the switch automatically takes a snapshot of the Junos OS root file system in the alternate root partition and copies it onto the primary root partition, thereby repairing the corrupt file in the primary root partition. The automatic snapshot procedure takes place whenever the system reboots from the alternate root partition, regardless of whether the reboot is due to a command or due to corruption of the primary root partition.

NOTE: **EX9200 switches do not support the automatic snapshot feature.**

Default

- The automatic snapshot feature is enabled by default on the following EX Series switches:
  - EX4550 switches
  - EX Series switches that ship with Junos OS Release 12.3R1 or later
- The automatic snapshot feature is disabled by default on EX Series switches (except the EX4550 switches) running Junos OS Release 12.2 or earlier.
- If the automatic snapshot feature was disabled by default before the switch was upgraded to Junos OS Release 12.3R1 or later, the feature remains disabled (for backward compatibility) by default after the upgrade.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Understanding Resilient Dual-Root Partitions on Switches on page 93
- **show system auto-snapshot on page 413**

autoinstallation

Syntax

```
autoinstallation {
  configuration-servers {
    url {
      password password;
    }
  }
  interfaces {
    interface-name {
      bootp;
      rarp;
    }
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the configuration for autoinstallation.

Options The remaining statements are explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Autoinstallation on J Series and SRX Series Devices on page 88
- *Installation and Upgrade Guide*

configuration-servers

Syntax

```
configuration-servers {
  url {
    password password;
  }
}
```

Hierarchy Level [edit system autoinstallation]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the URL address of a server from which the configuration files must be obtained.

Options

- **url**—Specify the URL address of the server containing the configuration files.
- ***password***—Specify the password for authentication with the configuration server.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Installation and Upgrade Guide*

interfaces (Autoinstallation)

Syntax

```
interfaces {
  interface-name {
    bootp;
    rarp;
  }
}
```

Hierarchy Level [edit system autoinstallation]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the interface on which to perform autoinstallation. A request for an IP address is sent from the interface. Specify the IP address procurement protocol.

Options

- **bootp**—Enables BOOTP or DHCP during autoinstallation.
- **rarp**—Enables RARP during autoinstallation.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Autoinstallation on J Series and SRX Series Devices on page 88
- *Installation and Upgrade Guide*

license

Syntax

```
license {
  autoupdate {
  url url;
  password password;
  }
  renew {
    before-expiration number;
    interval interval-hours;
  }
  traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify license information for the device.

Options

- **autoupdate**—Autoupdate license keys from license servers.
  - **url**—URL of a license server.
- **renew**—License renewal lead time and checking interval.
  - **before-expiration *number***—License renewal lead time before expiration in days.

    Range : 0 through 60 days
  - **interval *interval-hours***—License checking interval in hours.

    Range : 1 through 336 hours
- **traceoptions**—Set the trace options.
  - **file**—Configure the trace file information.
    - *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
    - **files *number***— Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** ***maximum file-size*** option.

Range : 2 through 1000 files

Default : 10 files

- **match** ***regular-expression***—Refine the output to include lines that contain the regular expression.
- **size** ***maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

  Range : 10 KB through 1 GB

  Default : 128 KB

  If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** ***number*** option.
- **(world-readable | no-world-readable)**— By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag** ***flag***—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.
  - **all**—Trace all operations
  - **config**—Trace license configuration processing.
  - **events**—Trace licensing events and their processing.
- **no-remote-trace**—Disable the remote tracing.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS License Overview for J Series and SRX Series Devices*
- *Installation and Upgrade Guide*

usb

Syntax

```
usb {
   disable;
}
```

Hierarchy Level [edit system autoinstallation]

Release Information Statement introduced before Junos OS Release 7.4.

Description Disable the USB autoinstallation process.

Options **disable**—Disable the process.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Autoinstallation on J Series and SRX Series Devices on page 88
- *Installation and Upgrade Guide*

CHAPTER 18

Operational Commands

- request system software rollback
- request system software rollback (Maintenance)
- request system software validate
- request system zeroize
- show chassis nonstop-upgrade node-group
- show chassis usb storage
- show system auto-snapshot
- show system autoinstallation status
- show system autorecovery state
- show system boot-messages
- show system auto-snapshot
- show system download
- show system license
- show system license (SRX Series Services Gateways)
- show system login lockout
- show system snapshot
- show system snapshot media
- request system software abort in-service-upgrade (ICU)
- show system storage partitions (EX Series Switches Only)
- show system storage partitions (View SRX Series)

clear system login lockout

Syntax

clear system login lockout
<all>
<user *username*>

Release Information

Command introduced in Junos OS Release 11.2.

Description

Unlock the user account locked as a result of invalid login attempts.

Options

all—Clear all locked user accounts.

user *username*—Clear the specified locked user account.

Required Privilege Level

clear

Related Documentation

- *lockout-period*
- show system login lockout on page 440

Output Fields

This command produces no output.

request system autorecovery state

Syntax request system autorecovery state (save | recover | clear)

Release Information Command introduced in Junos Release 11.2.

Description Prepares the system for autorecovery of configuration, licenses, and disk information.

Options **save**—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.

The active Junos OS configuration is saved as the Junos rescue configuration, after which the rescue configuration, licenses, and disk partitioning information is saved for autorecovery. Autorecovery information must be initially saved using this command for the autorecovery feature to verify integrity of data on every bootup.

NOTE:

- Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed.
- A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten.

recover—Recover the disk partitioning, configuration, and licenses.

After autorecovery data has been saved, the integrity of saved items is always checked automatically on every bootup. The recovery command allows you to forcibly re-run the tests at any time if required.

clear—Clear all saved autorecovery information.

Only the autorecovery information is deleted; the original copies of the data used by the router are not affected. Clearing the autorecovery information also disables all autorecovery integrity checks performed during bootup.

Required Privilege Level maintenance

Related Documentation

- show system autorecovery state on page 417
- *Installation and Upgrade Guide*

List of Sample Output

request system autorecovery state save on page 343
request system autorecovery state recover on page 343
request system autorecovery state clear on page 343

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system autorecovery state save

```
user@host> request system autorecovery state save
Saving config recovery information
      Saving license recovery information
      Saving bsdlabel recovery information
```

Sample Output

request system autorecovery state recover

```
user@host> request system autorecovery state recover

Configuration:
File             Recovery Information    Integrity Check    Action / Status
rescue.conf.gz   Saved                   Passed             None
Licenses:
File             Recovery Information    Integrity Check    Action / Status
JUNOS282736.lic  Saved                   Passed             None
JUNOS282737.lic  Saved                   Failed             Recovered
BSD Labels:
Slice            Recovery Information    Integrity Check    Action / Status
s1               Saved                   Passed             None
s2               Saved                   Passed             None
s3               Saved                   Passed             None
s4               Saved                   Passed             None
```

Sample Output

request system autorecovery state clear

```
user@host> request system autorecovery state clear
Clearing config recovery information
       Clearing license recovery information
       Clearing bsdlabel recovery information
```

request system download abort

Syntax request system download abort *<download-id>*

Release Information Command introduced in Release 11.2 of Junos OS.

Description Abort a download. The download instance is stopped and cannot be resumed. Any partially downloaded file is automatically deleted to free disk space. Information regarding the download is retained and can be displayed with the **show** command until a Clear operation is performed.

NOTE: **Only downloads in the active, paused, and error states can be aborted.**

Options **download-id**—(Required) The ID number of the download to be paused.

Required Privilege Level maintenance

Related Documentation

- request system download start on page 348
- request system download pause on page 346
- request system download resume on page 347
- request system download clear on page 345
- *Installation and Upgrade Guide*

List of Sample Output request system download abort on page 344

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download abort

```
user@host> request system download abort 1
Aborted download #1
```


request system download clear

Syntax request system download clear

Release Information Command introduced in Release 11.2 of Junos OS.

Description Delete the history of completed and aborted downloads.

Required Privilege Level maintenance

Related Documentation

- request system download start on page 348
- request system download pause on page 346
- request system download resume on page 347
- request system download abort on page 344
- *Installation and Upgrade Guide*

List of Sample Output request system download clear on page 345

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download clear

```
user@host> request system download clear
Cleared information on completed and aborted downloads
```

request system download pause

Syntax request system download pause <*download-id*>

Release Information Command introduced in Release 11.2 of Junos OS.

Description Suspend a particular download instance.

NOTE: **Only downloads in the active state can be paused.**

Options **download-id**—(Required) The ID number of the download to be paused.

Required Privilege Level maintenance

Related Documentation

- request system download start on page 348
- request system download resume on page 347
- request system download abort on page 344
- request system download clear on page 345
- *Installation and Upgrade Guide*

List of Sample Output request system download pause on page 346

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download pause

```
user@host> request system download pause 1
Paused download #1
```

request system download resume

Syntax request system download resume *download-id* <max-rate>

Release Information Command introduced in Release 11.2 of Junos OS.

Description Resume a download that has been paused. Download instances that are not in progress because of an error or that have been explicitly paused by the user can be resumed by the user. The file will continue downloading from the point where it paused. By default, the download resumes with the same bandwidth specified with the **request system download start** command. The user can optionally specify a new (maximum) bandwidth with the **request system download resume** command.

NOTE: **Only downloads in the paused and error states can be resumed.**

Options **download-id**—(Required) The ID number of the download to be paused.

max-rate—(Optional) The maximum bandwidth for the download.

Required Privilege Level maintenance

Related Documentation

- request system download start on page 348
- request system download pause on page 346
- request system download abort on page 344
- request system download clear on page 345
- *Installation and Upgrade Guide*

List of Sample Output request system download resume on page 347

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download resume

```
user@host> request system download resume 1
Resumed download #1
```

request system download start

Syntax request system download start (*url* | *max-rate* | *save as* | *login* | *delay*)

Release Information Command introduced in Release 11.2 of Junos OS.

Description Creates a new download instance and identifies it with a unique integer called the download ID.

Options **url**—(Required) The FTP or HTTP URL location of the file to be downloaded.

max-rate—(Optional) The maximum average bandwidth for the download. Numbers with the suffix k or K, m or M, and g or G are interpreted as kbps, mbps, or gbps, respectively.

save-as—(Optional) The filename to be used for saving the file in the **/var/tmp** location.

login—(Optional) The username and password for the server in the format **username:password**.

delay—(Optional) The number of hours after which the download should start.

Required Privilege Level maintenance

Related Documentation

- request system download pause on page 346
- request system download resume on page 347
- request system download abort on page 344
- request system download clear on page 345
- *Installation and Upgrade Guide*

List of Sample Output request system download start on page 348

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download start

```
user@host> request system download start login user:passwd ftp://ftp-server//tftpboot/1m_file
max-rate 1k
Starting download #1
```


request system firmware upgrade

Syntax request system firmware upgrade

Release Information Command introduced in Release 10.2 of Junos OS.

Description Upgrade firmware on a system.

Options **fpc**—Upgrade FPC ROM monitor.

pic—Upgrade PIC firmware.

re—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.

vcpu—Upgrade VCPU ROM monitor.

Required Privilege Level maintenance

Related Documentation
- *Installation and Upgrade Guide*

List of Sample Output request system firmware upgrade on page 349

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system firmware upgrade

```
user@host> request system firmware upgrade re bios
Part             Type           Tag Current   Available Status
                                    version   version
Routing Engine 0 RE BIOS        0   1.5       1.9       OK
Routing Engine 0 RE BIOS Backup 1   1.7       1.9       OK
Perform indicated firmware upgrade ? [yes,no] (no) yes
```

```
user@host> request system firmware upgrade re bios backup
Part             Type           Tag Current   Available Status
                                    version   version
Routing Engine 0 RE BIOS        0   1.5       1.9       OK
Routing Engine 0 RE BIOS Backup 1   1.7       1.9       OK
Perform indicated firmware upgrade ? [yes,no] (no) yes
```

request system license add

Syntax request system license add (*filename* | terminal)

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 9.5 for SRX Series devices.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Add a license key.

Options ***filename***—License key from a file or URL. Specify the filename or the URL where the key is located.

terminal—License key from the terminal.

Required Privilege Level maintenance

Related Documentation
- Adding New Licenses (CLI Procedure) on page 313

List of Sample Output request system license add on page 350

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license add

```
user@host> request system license add terminal
E408408918 aeaqib qcsbja okbuqe rcmxnq vjocwf uxfsta
           z5ufjb kdrmt6 57bimv 2f3ddp qttcdn 627q4a
           jx4s5x hiri
E408408918: successfully added
add license complete (no errors)
```


request system license delete

Syntax

request system license delete (*license-identifier* | license-identifier-list [*licenseid001 licenseid002 licenseid003*]| all)

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Option **license-identifier-list** introduced in Junos OS Release 13.1.

Description

Delete a license key. You can choose to delete one license at a time, all licenses at once, or a list of license identifiers enclosed in brackets.

Options

license-identifier—Text string that uniquely identifies a license key.

license-identifier-list [***licenseid001 licenseid002 licenseid003....*** **]**—Delete multiple license identifiers as a list enclosed in brackets.

all—Delete all licenses on the device.

Required Privilege Level

maintenance

Related Documentation

- Deleting a License (CLI Procedure) on page 314

request system license save

Syntax request system license save (*filename* | terminal)

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 9.5 for SRX Series devices.

Description Save installed license keys to a file or URL.

Options ***filename***—License key from a file or URL. Specify the filename or the URL where the key is located.

terminal—License key from the terminal.

Required Privilege Level maintenance

Related Documentation
- Saving License Keys on page 315

List of Sample Output request system license save on page 352

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license save

```
user@host> request system license save ftp://user@host/license.conf
```


request system license update

Syntax request system license update

Release Information Command introduced in Release 9.5 of Junos OS.

Description Starts autoupdating license keys from the LMS server.

This command is supported on J-series devices.

Options **trial**—Starts autoupdating trial license keys from LMS server.

Required Privilege Level maintenance

List of Sample Output request system license update on page 353
request system license update trial on page 353

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license update

```
user@host> request system license update

Trying to update license keys from https://ae1.juniper.net has been sent, use
show system license to check status.
```

request system license update trial

```
user@host> request system license update trial

Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

request system partition compact-flash

Syntax request system partition compact-flash

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reboots the device and repartitions the compact flash. The compact flash is repartitioned only if it is possible to restore all the data on the compact flash. Otherwise, the operation is aborted, and a message is displayed indicating that the current disk usage needs to be reduced.

Required Privilege Level maintenance

List of Sample Output request system partition compact-flash (If Yes) on page 354
request system partition compact-flash (If No) on page 354

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system partition compact-flash (If Yes)

```
user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] yes
Initiating repartition operation.
The operation may take several minutes to complete.
System will reboot now...
<System reboots>
<Repartition operation is performed>
<System reboots and starts up normally>
```

Sample Output

request system partition compact-flash (If No)

```
user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] no
```


request system reboot

List of Syntax

Syntax on page 355
Syntax (EX Series Switches) on page 355
Syntax (TX Matrix Router) on page 355
Syntax (TX Matrix Plus Router) on page 355
Syntax (MX Series Router) on page 355

Syntax

request system reboot
<at *time*>
<both-routing-engines>
<in *minutes*>
<media (compact-flash | disk | removable-compact-flash | usb)>
<message "*text*">
<other-routing-engine>

Syntax (EX Series Switches)

request system reboot
<all-members>
<at *time*>
<both-routing-engines>
<in *minutes*>
<local>
<media (external | internal)>
<member *member-id*>
<message "*text*">
<other-routing-engine>
<slice *slice*>

Syntax (TX Matrix Router)

request system reboot
<all-chassis | all-lcc | lcc *number* | scc>
<at *time*>
<both-routing-engines>
<in *minutes*>
<media (compact-flash | disk)>
<message "*text*">
<other-routing-engine>

Syntax (TX Matrix Plus Router)

request system reboot
<all-chassis | all-lcc | lcc *number* | sfc *number*>
<at *time*>
<both-routing-engines>
<in *minutes*>
<media (compact-flash | disk)>
<message "*text*">
<other-routing-engine>
<partition (1 | 2 | alternate)>

Syntax (MX Series Router)

request system reboot
<all-members>
<at *time*>
<both-routing-engines>
<in *minutes*>
<local>

<media (external | internal)>
<member *member-id*>
<message "*text*">
<other-routing-engine>

Release Information Command introduced before Junos OS Release 7.4.
Option **other-routing-engine** introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Option **both-routing-engines** introduced in Junos OS Release 12.1.

Description Reboot the software.

Options **none**—Reboot the software immediately.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.

all-lcc—(TX Matrix routers andTX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.

all-members—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on all members of the Virtual Chassis configuration.

at *time*—(Optional) Time at which to reboot the software, specified in one of the following ways:

- **now**—Stop or reboot the software immediately. This is the default.
- ***+minutes***—Number of minutes from now to reboot the software.
- ***yymmddhhmm***—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
- ***hh:mm***—Absolute time on the current day at which to stop the software, specified in 24-hour time.

both-routing-engines—(Optional) Reboot both Routing Engines at the same time.

in *minutes*—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at *+minutes*** option.

lcc *number*——(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.

- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the local Virtual Chassis member.

media (compact-flash | disk | removable-compact-flash | usb)—(Optional) Boot medium for next boot. (The options **removable-compact-flash** and **usb** pertain to the J Series routers only.)

media (external | internal)—(EX Series switches and MX Series routers only) (Optional) Reboot the boot media:

- **external**—Reboot the external mass storage device.
- **internal**—Reboot the internal flash device.

member *member-id*—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace ***member-id*** with a value from 0 through 9. For an MX Series Virtual Chassis, replace ***member-id*** with a value of 0 or 1.

message "*text*"—(Optional) Message to display to all system users before stopping or rebooting the software.

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

partition—(TX Matrix Plus routers only) (Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:

- **1**—Reboot from partition 1.
- **2**—Reboot from partition 2.
- **alternate**—Reboot from the alternate partition.

scc—(TX Matrix routers only) (Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted.

sfc *number*—(TX Matrix Plus routers only) (Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace *number* with 0.

slice *slice*—(EX Series switches only) (Optional) Reboot a partition on the boot media. This option has the following suboptions:

- **1**—Power off partition 1.
- **2**—Power off partition 2.
- **alternate**—Reboot from the alternate partition.

Additional Information

Reboot requests are recorded in the system log files, which you can view with the **show log** command (see *show log*). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the **show system processes** command (see *show system processes*).

On a TX Matrix or TX Matrix Plus router, if you issue the **request system reboot** command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.

NOTE: Before issuing the **request system reboot** command on a TX Matrix Plus router with no options or the **all-chassis**, **all-lcc**, **lcc** *number*, or **sfc** options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the **request system reboot** command.

NOTE: To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

Required Privilege Level

maintenance

Related Documentation

- *clear system reboot*
- *request system halt*
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

List of Sample Output

request system reboot on page 359
request system reboot (at 2300) on page 359
request system reboot (in 2 Hours) on page 359
request system reboot (Immediately) on page 359
request system reboot (at 1:20 AM) on page 359

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@host> request system reboot
Reboot the system ? [yes,no] (no)
```

request system reboot (at 2300)

```
user@host> request system reboot at 2300 message ?Maintenance time!?
Reboot the system ? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00
```

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

```
user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00
```

request system reboot (Immediately)

```
user@host> request system reboot at now
```

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

```
user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
```

request system reboot

Syntax

request system reboot
<all-members | local | member **member-id**>
<at **time**>
<in **minutes**>
<media (external | internal)>
<message "**text**">
<slice (1 | 2 | alternate)>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **partition** changed to **slice** in Junos OS Release 10.0 for EX Series switches.

Description

Reboot the Junos OS.

Reboot requests are recorded in the system log files, which you can view with the **show log** command. You can view the process names with the **show system processes** command.

Options

none—Reboots the software immediately.

all-members | local | member *member-id*—(EX4200 switch only) (Optional) Specify which member of the Virtual Chassis to reboot:

- **all-members**—Reboots each switch that is a member of the Virtual Chassis.
- **local**—Reboots the local switch, meaning the switch you are logged into, only.
- **member *member-id***—Reboots the specified member switch of the Virtual Chassis.

at time—(Optional) Time at which to reboot the software, specified in one of the following ways:

- ***+minutes***—Number of minutes from now to reboot the software.
- ***hh:mm***—Absolute time on the current day at which to reboot the software, specified in 24-hour time.
- **now**—Stop or reboot the software immediately. This is the default.
- ***yymmddhhmm***—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.

in minutes—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at *+minutes*** option.

media (external | internal)—(Optional) Boot medium for the next boot. The external option reboots the switch using a software package stored on an external boot source, such as a USB flash drive. The internal option reboots the switch using a software package stored in an internal memory source.

message "text"—(Optional) Message to display to all system users before rebooting the software.

slice (1 | 2 | alternate)—(Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:

- **1**—Reboot from partition 1.
- **2**—Reboot from partition 2.
- **alternate**—Reboot from the alternate partition, which is the partition that did not boot the switch at the last bootup.

Required Privilege Level maintenance

Related Documentation

- *clear system reboot*

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@host> request system reboot
Reboot the system ? [yes,no] (no)
```

request system reboot (at 2300)

```
user@host> request system reboot at 2300 message ?Maintenance time!?
Reboot the system ? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00
```

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

```
user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00
```

request system reboot (Immediately)

```
user@host> request system reboot at now
```

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

```
user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
```

request system scripts add

Syntax

request system scripts add *<package-name>*
<no-copy>
<unlink>

Release Information

Command introduced before Junos OS Release 9.0.

Description

CLI command to install AI-Script (jais) packages on Juniper Networks devices.

Options

no-copy—Don't save a copy of the jais package file.

user@host> **request system scripts add no-copy** *<package-name>*

NOTE: **If you use the no-copy option during the jais installation, the jais package cannot be rolled back.**

unlink—Remove the package after successful installation.

user@host> **request system scripts add unlink** *<package-name>*

Required Privilege Level

maintenance

Related Documentation

- request system scripts delete on page 363
- request system scripts rollback on page 364
- *request system scripts event-scripts*

request system scripts delete

Syntax **request system scripts delete** *<package-name>*

Release Information Command introduced before Junos OS Release 9.0.

Description CLI command to delete AI-Script (jais) packages on Juniper Networks devices.

Options No options are available.

Required Privilege Level maintenance

Related Documentation

- request system scripts add on page 362
- request system scripts rollback on page 364
- *request system scripts event-scripts*

request system scripts rollback

Syntax **request system scripts rollback**

Release Information Command introduced before Junos OS Release 9.0.

Description Attempt to roll back to most recent installation of AI-Scripts (jais) package.

Options No options are available.

Required Privilege Level maintenance

Related Documentation

- request system scripts add on page 362
- request system scripts delete on page 363
- *request system scripts event-scripts*

request system snapshot

List of Syntax

Syntax

request system snapshot
<partition>

Syntax (ACX Series Routers)

request system snapshot
<media *type*>
<partition>

Syntax (EX Series Switches)

request system snapshot
<all-members | local | member *member-id*>
<media *type*>
<partition>
<re0 | re1 | routing-engine *routing-engine-id*>
<slice alternate>

Syntax (MX Series Routers)

request system snapshot
<all-members>
<config-partition>
<local>
<member *member-id*>
<media *usb-port-number*>
<partition>
<root-partition>

Syntax (TX Matrix Routers)

request system snapshot
<all-chassis | all-lcc | lcc *number* | scc>
<config-partition>
<partition>
<root-partition>

Syntax (TX Matrix Plus Routers)

request system snapshot
<all-chassis | all-lcc | lcc *number* | sfc *number*>
<config-partition>
<partition>
<root-partition>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 12.2 for ACX Series switches.
Options **<config-partition>** and **<root-partition>** introduced in Junos OS Release 13.1 for M, MX, T, TX Series switches.
Option **media *usb-port-number*** introduced in Junos OS Release 13.2 for MX104 routers.

Description

- On the router, back up the currently running and active file system partitions to standby partitions that are not running. Specifically, the root file system (/) is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.
- On the switch, take a snapshot of the files currently used to run the switch—the complete contents of the root (/) , **/altroot**, **/config**, **/var**, and **/var-tmp** directories, which include the running Junos OS, the active configuration, and log files.

CAUTION: **After you run the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.**

Options The specific options available depend upon the router or switch:

none—Back up the currently running software as follows:

- On the router, back up the currently running and active file system partitions to standby partitions that are not running. Specifically, the root file system (/) is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.
- On the switch, take a snapshot of the files currently used to run the switch and copy them to the media that the switch did not boot from. If the switch is booted from internal media, the snapshot is copied to external (USB) media. If the switch is booted from external (USB) media, the snapshot is copied to internal media.
  - If the snapshot destination is external media but a USB flash drive is not connected, an error message is displayed.
  - If the automatic snapshot procedure is already in progress, the command returns the following error: **Snapshot already in progress. Cannot start manual snapshot.** For additional information about the automatic snapshot feature, see "Understanding Resilient Dual-Root Partitions on Switches" on page 93.

all-chassis | all-lcc | lcc *number* —(TX Matrix and TX Matrix Plus router only) (Optional)

- **all-chassis**—On a TX Matrix router, archive data and executable areas for all Routing Engines in the chassis. On a TX Matrix Plus router, archive data and executable areas for all Routing Engines in the chassis.
- **all-lcc**—On a TX Matrix router, archive data and executable areas for all T640 routers (or line-card chassis) connected to a TX Matrix router. On a TX Matrix Plus router, archive data and executable areas for all routers (or line-card chassis) connected to a TX Matrix Plus router.
- **lcc *number***—On a TX Matrix router, archive data and executable areas for a specific T640 router (or line-card chassis) that is connected to a TX Matrix router. On a

TX Matrix Plus router, archive data and executable areas for a specific router (line-card chassis) that is connected to a TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

all-members | local | member *member-id*—(EX Series switch Virtual Chassis and MX Series routers only) (Optional) Specify where to place the snapshot (archive data and executable areas) in a Virtual Chassis:

- **all-members**—Create a snapshot (archive data and executable areas) for all members of the Virtual Chassis.
- **local**—Create a snapshot (archive data and executable areas) on the member of the Virtual Chassis that you are currently logged into.
- **member *member-id***—Create a snapshot (archive data and executable areas) for the specified member of the Virtual Chassis.

config-partition—(M, MX, T, TX Series routers only) Create a snapshot of the configuration partition only and store it onto the default **/altconfig** on the hard disk device or an **/altconfig** on a USB device.

media *type*—(ACX Series, M320, T640, MX960 routers, and EX Series switches only)(Optional) Specify the boot device the software is copied to:

- **compact-flash**—Copy software to the primary compact flash drive.
- **external**—(Switches only) Copy software to an external mass storage device, such as a USB flash drive. If a USB drive is not connected, the switch displays an error message.
- **internal**—Copy software to an internal flash drive.
- **removable-compact-flash**—Copy software to the removable compact flash drive.
- **usb**—(ACX Series, M320, T640, MX960 routers only) Copy software to the device connected to the USB port.
- **usb0**—(MX104 routers only) Copy software to the device connected to the USB0 port.
- **usb1**—(MX104 routers only) Copy software to the device connected to the USB1 port.

partition—(Optional) Repartition the flash drive before a snapshot occurs. If the partition table on the flash drive is corrupted, the **request system snapshot** command fails and reports errors. The partition option is only supported for restoring the software image from the hard drive to the flash drive.

(Routers only) You cannot issue the request system snapshot command when you enable flash disk mirroring. We recommend that you disable flash disk mirroring when you upgrade or downgrade the software. For more information, see the *Junos OS Administration Library for Routing Devices*.

(EX Series switches only) If the snapshot destination is the media that the switch did not boot from, you must use the **partition** option.

re0 | re1 | routing-engine ***routing-engine-id***—(EX6200 and EX8200 switches only) Specify where to place the snapshot in a redundant Routing Engine configuration.

- **re0**—Create a snapshot on Routing Engine 0.
- **re1**—Create a snapshot on Routing Engine 1.
- **routing-engine** *routing-engine-id*—Create a snapshot on the specified Routing Engine.

root-partition—(M, MX, T, TX Series routers only) Create a snapshot of the root partition only and store it onto the default **/altroot** on the hard disk device or an **/altroot** on a USB device.

slice alternate—(EX Series switches only) (Optional) Take a snapshot of the active root partition and copy it to the alternate slice on the boot media.

scc—(TX Matrix router only) (Optional) Archive data and executable areas for a TX Matrix router (or switch-card chassis).

sfc ***number***—(TX Matrix Plus router only) (Optional) Archive data and executable areas for a TX Matrix Plus router (or switch-fabric chassis). Replace *number* with 0.

Additional Information

- (Routers only) Before upgrading the software on the router, when you have a known stable system, issue the **request system snapshot** command to back up the software, including the configuration, to the **/altroot** and **/altconfig** file systems. After you have upgraded the software on the router and are satisfied that the new packages are successfully installed and running, issue the **request system snapshot** command again to back up the new software to the **/altroot** and **/altconfig** file systems.
- (Routers only) You cannot issue the **request system snapshot** command when you enable flash disk mirroring. We recommend that you disable flash disk mirroring when you upgrade or downgrade the software. For more information, see the *Junos OS Administration Library for Routing Devices*
- (TX Matrix and TX Matrix Plus router only) On a routing matrix, if you issue the **request system snapshot** command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are backed up. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are backed up.

Required Privilege Level maintenance

Related Documentation
- show system snapshot on page 441
- show system auto-snapshot on page 413

List of Sample Output

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system snapshot (Routers)

```
user@host> request system snapshot
umount: /altroot: not currently mounted
Copying / to /altroot.. (this may take a few minutes)
umount: /altconfig: not currently mounted
Copying /config to /altconfig.. (this may take a few minutes)

The following filesystems were archived: / /config
```

request system snapshot (EX Series Switches)

```
user@switch> request system snapshot partition
Clearing current label...
Partitioning external media (/dev/da1) ...
Partitions on snapshot:

  Partition  Mountpoint  Size    Snapshot argument
      s1a    /altroot    179M    none
      s2a    /           180M    none
      s3d    /var/tmp    361M    none
      s3e    /var        121M    none
      s4d    /config     60M     none
Copying '/dev/da0s1a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2a' to '/dev/da1s2a' .. (this may take a few minutes)
Copying '/dev/da0s3d' to '/dev/da1s3d' .. (this may take a few minutes)
Copying '/dev/da0s3e' to '/dev/da1s3e' .. (this may take a few minutes)
Copying '/dev/da0s4d' to '/dev/da1s4d' .. (this may take a few minutes)
The following filesystems were archived: /altroot / /var/tmp /var /config
```

request system snapshot (When the Partition Flag Is On)

```
user@host> request system snapshot partition
Performing preliminary partition checks ...
Partitioning ad0 ...
umount: /altroot: not currently mounted
Copying / to /altroot.. (this may take a few minutes)

The following filesystems were archived: / /config
```

request system snapshot (MX104 routers when media device is missing)

```
user@host > request system snapshot media usb0
error: usb0 media missing or invalid
```

request system snapshot (When Mirroring Is Enabled)

```
user@host> request system snapshot
Snapshot is not possible since mirror-flash-on-disk is configured.
```

request system snapshot all-lcc (Routing Matrix)

```
user@host> request system snapshot all-lcc
lcc0-re0:
--------------------------------------------------------------------------
Copying '/' to '/altroot' .. (this may take a few minutes)
Copying '/config' to '/altconfig' .. (this may take a few minutes)
The following filesystems were archived: / /config

lcc2-re0:
--------------------------------------------------------------------------
Copying '/' to '/altroot' .. (this may take a few minutes)
Copying '/config' to '/altconfig' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system snapshot all-members (Virtual Chassis)

```
user@switch> request system snapshot all-members media internal
fpc0:
--------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc1:
--------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc2:
--------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc3:
--------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc4:
--------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc5:
--------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /
```

request system snapshot (Maintenance)

Syntax request system snapshot

Release Information Command introduced in Release 10.2 of Junos OS.

Description Back up the currently running and active file system partitions on the device.

Options

- **factory**— (Optional) Specifies that only the files shipped from the factory are included in the snapshot.
- **media**— (Optional) Specifies the media to be included in the snapshot:
  - **internal**— Copies the snapshot to internal media. This is the default.
  - **usb**— Copies the snapshot to the USB storage device.
  - **external**— Copies the snapshot to an external storage device. This option is available for the compact flash on the SRX650 Services Gateway.
- **partition** - (Default) Specifies that the target media should be repartitioned before the backup is saved to it.

  NOTE: The target media is partitioned whether or not it is specified in the command, because this is a mandatory option.

- **slice**— (Optional) Takes a snapshot of the root partition the system has currently booted from to another slice in the same media.
  - alternate— (Optional) Stores the snapshot on the other root partition in the system.

  NOTE: The slice option cannot be used along with the other **request system snapshot** options, because the options are mutually exclusive. If you use the factory, media, or partition option, you cannot use the slice option; if you use the slice option, you cannot use any of the other options.

Required Privilege Level maintenance

Related Documentation

- *Installation and Upgrade Guide*

Example

```
user@host# request system snapshot media usb partition

user@host# request system snapshot media usb partition factory
```

request system software abort in-service-upgrade (ICU)

Syntax request system software abort in-service-upgrade

Release Information Command introduced in Release 11.2 of Junos OS.

Description Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the **request system in-service-upgrade** command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.

Options This command has no options.

Required Privilege Level view

Related Documentation

- *request system software in-service-upgrade (Maintenance)*

List of Sample Output request system software abort in-service-upgrade on page 372

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software abort in-service-upgrade

```
user@host> request system software abort in-service-upgrade
In-Service-Upgrade aborted
```


request system software add

List of Syntax

Syntax

request system software add *package-name*
<best-effort-load>
<delay-restart>
<force>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<set [*package-name package-name*]>
<unlink>
<upgrade-with-config>
<upgrade-with-config-format *format*>
<validate>

Syntax (EX Series Switches)

request system software add *package-name*
<best-effort-load>
<delay-restart>
<force>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<set [*package-name package-name*]>
<upgrade-with-config>
<upgrade-with-config-format *format*>
<validate>

Syntax (TX Matrix Router)

request system software add *package-name*
<best-effort-load>
<delay-restart>
<force>
<lcc *number* | scc>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<set [*package-name package-name*]>
<unlink>
<upgrade-with-config>
<upgrade-with-config-format *format*>
<validate>

Syntax (TX Matrix Plus Router)

request system software add *package-name*
<best-effort-load>
<delay-restart>
<force>
<lcc *number* | sfc *number*>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<set [*package-name package-name*]>
<unlink>
<upgrade-with-config>
<upgrade-with-config-format *format*>
<validate>

Syntax (MX Series Router)

request system software add *package-name*
<best-effort-load>
<delay-restart>
<force>
<member *member-id*>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<set [*package-name package-name*]>
<unlink>
<upgrade-with-config>
<upgrade-with-config-format *format*>
<validate>

Syntax (QFX Series)

request system software add *package-name*
<best-effort-load>
<component all>
<delay-restart>
<force>
<force-host>
<no-copy>
<no-validate>
<partition>
<reboot>
<unlink>
<upgrade-with-config>
<upgrade-with-config-format *format*>
<validate>

Syntax (OCX Series)

request system software add *package-name*
<best-effort-load>
<delay-restart>
<force>
<force-host>
<no-copy>
<no-validate>
<reboot>
<unlink>
<upgrade-with-config>

<upgrade-with-config-format *format*>
<validate>

Release Information

Command introduced before Junos OS Release 7.4.
best-effort-load and **unlink** options added in Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
set [*package-name package-name*] option added in Junos OS Release 11.1 for EX Series switches.
set [*package-name package-name*] option added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways.

NOTE: On EX Series switches, the **set [*package-name package-name*]** option allows you to install only two software packages on a mixed EX4200 and EX4500 Virtual Chassis, whereas, on M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways, the **set [*package-name package-name*]** option allows you to install multiple software packages and software add-on packages at the same time.

upgrade-with-config and **upgrade-with-config-format *format*** options added in Junos OS Release 12.3 for M Series routers, MX Series routers, T Series routers, EX Series Ethernet switches, and QFX Series devices.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

NOTE: We recommend that you always download the software image to **/var/tmp** only. On EX Series and QFX Series switches, you must use the **/var/tmp** directory. Other directories are not supported.

Install a software package or bundle on the router or switch.

WARNING: Any configuration changes performed after inputting the **request system software add** command will be lost when the system reboots with an upgraded version of JUNOS.

Options

package-name—Location from which the software package or bundle is to be installed. For example:

- ***/var/tmp/package-name***—For a software package or bundle that is being installed from a local directory on the router or switch.
- ***protocol://hostname/pathname/package-name***—For a software package or bundle that is to be downloaded and installed from a remote location. Replace ***protocol*** with one of the following:

- **ftp**—File Transfer Protocol.
  Use **ftp***://hostname/pathname/package-name*. To specify authentication credentials, use **ftp***://<username>:<password>@hostname/pathname/package-name*. To have the system prompt you for the password, specify **prompt** in place of the password. If a password is required, and you do not specify the password or **prompt**, an error message is displayed.
- **http**—Hypertext Transfer Protocol.
  Use **http***://hostname/pathname/package-name*. To specify authentication credentials, use **http***://<username>:<password>@hostname/pathname/package-name*. If a password is required and you omit it, you are prompted for it.
- **scp**—Secure copy (available only for Canada and U.S. version).
  Use **scp***://hostname/pathname/package-name*. To specify authentication credentials, use **scp***://<username>:<password>@hostname/pathname/package-name*.

NOTE:

- The *pathname* in the protocol is the relative path to the user's home directory on the remote system and not the root directory.
- Do not use the **scp** protocol in the **request system software add** command to download and install a software package or bundle from a remote location. The previous statement does not apply to the QFabric switch. The software upgrade is handled by the MGD process which does not support scp.
  Use the **file copy** command to copy the software package or bundle from the remote location to the **/var/tmp** directory on the hard disk:
  file copy scp*://source/package-name* **/var/tmp**
  Then install the software package or bundle using the **request system software add** command:
  request system software add /var/tmp*/package-name*
- On a J Series Services Router, when you install the software from a remote location, the package is removed at the earliest opportunity in order to make room for the installation to be completed. If you copy the software to a local directory on the router and then install the new package, use the **unlink** option to achieve the same effect and allow the installation to be completed.

best-effort-load—(Optional) Activate a partial load and treat parsing errors as warnings instead of errors.

component all—(QFabric systems only) (Optional) Install software package on all of the QFabric components.

delay-restart—(Optional) Install a software package or bundle, but do not restart software processes.

force—(Optional) Force the addition of the software package or bundle (ignore warnings).

force-host—(Optional) Force the addition of host software package or bundle (ignore warnings) on the QFX5100 device.

lcc ***number*** —(TX Matrix routers and TX Matrix Plus routers only) (Optional) In a routing matrix based on the TX Matrix router, install a software package or bundle on a T640 router that is connected to the TX Matrix router. In a routing matrix based on the TX Matrix Plus router, install a software package or bundle on a router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

member ***member-id***—(MX Series routers only) (Optional) Install a software package on the specified Virtual Chassis member. Replace ***member-id*** with a value of 0 or 1.

partition —(QFX3500 switches only) (Optional) Format and repartition the media before installation.

scc—(TX Matrix routers only) (Optional) Install a software package or bundle on a Routing Engine on a TX Matrix router (or switch-card chassis).

sfc ***number***—(TX Matrix Plus routers only) (Optional) Install a software package or bundle on a Routing Engine on a TX Matrix Plus router. Replace *number* with 0.

no-copy—(Optional) Install a software package or bundle, but do not save copies of the package or bundle files.

no-validate—(Optional) When loading a software package or bundle with a different release, suppress the default behavior of the **validate** option.

re0 | re1—(Optional) On routers or switches that support dual or redundant Routing Engines, load a software package or bundle on the Routing Engine in slot 0 (re0) or the Routing Engine in slot 1 (re1).

reboot—(Optional) After adding the software package or bundle, reboot the system. On a QFabric switch, the software installation is not complete until you reboot the component for which you have installed the software.

set [*package-name package-name*]—(Mixed EX4200 and EX4500 Virtual Chassis only) (Optional) Install two software packages—a package for an EX4200 switch and the same release of the package for an EX4500 switch—to upgrade all member switches in a mixed EX4200 and EX4500 Virtual Chassis.

set [*package-name package-name*]—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages and software add-on packages at the same time.

unlink—(Optional) On J Series Services Routers, this option ensures that the software package is removed at the earliest opportunity in order to make room for the installation to be completed. On M Series, T Series, and MX Series routers, use the **unlink** option to remove the software package from this directory after a successful upgrade is completed.

upgrade-with-config—(Optional) Install one or more configuration files.

upgrade-with-config-format *format*—(Optional) Specify the configuration file fomat, **text** or **xml**. The default format is **text**.

NOTE: The **upgrade-with-config** and **upgrade-with-config-format** options are only available locally on the router or switch. In a routing matrix, the configuration is applied only to the local router and is not propagated to other routers.

The options are validated during the validation process and applied to the router or switch during the upgrade process. If the upgrade process is successful, the options are removed from the configuration. If the upgrade process fails, the configuration file is renamed with the .failed suffix.

validate—(Optional) Validate the software package or bundle against the current configuration as a prerequisite to adding the software package or bundle. This is the default behavior when the software package or bundle being added is a different release.

NOTE: The **validate** option only works on systems that do not have **graceful-switchover** (GRES) enabled. To use the **validate** option on a system with GRES, either disable GRES for the duration of the installation, or install using the command **request system software in-service-upgrade**, which requires nonstop active routing (NSR) to be enabled when using GRES.

Additional Information

Before upgrading the software on the router or switch, when you have a known stable system, issue the **request system snapshot** command to back up the software, including

the configuration, to the **/altroot** and **/altconfig** file systems. After you have upgraded the software on the router or switch and are satisfied that the new package or bundle is successfully installed and running, issue the **request system snapshot** command again to back up the new software to the **/altroot** and **/altconfig** file systems.

NOTE: The **request system snapshot** command is currently not supported on the QFabric system. Also, you cannot add or install multiple packages on a QFabric system.

After you run the **request system snapshot** command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

If you are upgrading more than one package at the same time, delete the operating system package, jkernel, last. Add the operating system package, jkernel, first and the routing software package, jroute, last. If you are upgrading all packages at once, delete and add them in the following order:

```
user@host> request system software add /var/tmp/jbase
user@host> request system software add /var/tmp/jkernel
user@host> request system software add /var/tmp/jpfe
user@host> request system software add /var/tmp/jdocs
user@host> request system software add /var/tmp/jroute
user@host> request system software add /var/tmp/jcrypto
```

By default, when you issue the **request system software add** ***package-name*** command on a TX Matrix master Routing Engine, all the T640 master Routing Engines that are connected to it are upgraded to the same version of software. If you issue the same command on the TX Matrix backup Routing Engine, all the T640 backup Routing Engines that are connected to it are upgraded to the same version of software.

Likewise, when you issue the **request system software add** ***package-name*** command on a TX Matrix Plus master Routing Engine, all the T1600 or T4000 master Routing Engines that are connected to it are upgraded to the same version of software. If you issue the same command on the TX Matrix Plus backup Routing Engine, all the T1600 or T4000 backup Routing Engines that are connected to it are upgraded to the same version of software.

Required Privilege Level

maintenance

Related Documentation

- request system software delete on page 385
- request system software rollback on page 397
- *request system storage cleanup*
- Upgrading Software on page 112
- Upgrading Software on a QFabric System on page 150

- request system software add (Maintenance) on page 382
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

List of Sample Output

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software add validate

```
user@host> request system software add validate /var/tmp/ jinstall-7.2R1.7-domestic-signed.tgz
Checking compatibility with configuration
Initializing...
Using jbase-7.1R2.2
Using /var/tmp/jinstall-7.2R1.7-domestic-signed.tgz
Verified jinstall-7.2R1.7-domestic.tgz signed by PackageProduction_7_2_0
Using /var/validate/tmp/jinstall-signed/jinstall-7.2R1.7-domestic.tgz
Using /var/validate/tmp/jinstall/jbundle-7.2R1.7-domestic.tgz
Checking jbundle requirements on /
Using /var/validate/tmp/jbundle/jbase-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jkernel-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jcrypto-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jpfe-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jdocs-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jroute-7.2R1.7.tgz
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Validating against /config/rescue.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/var/tmp/jinstall-7.2R1.7-domestic-signed.tgz' ...
Verified jinstall-7.2R1.7-domestic.tgz signed by PackageProduction_7_2_0
Adding jinstall...

WARNING:     This package will load JUNOS 7.2R1.7 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.

Saving the config files ...
Installing the bootstrap installer ...

WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software delete jinstall'
WARNING:     command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-7.2R1.7-domestic-signed.tgz ...
Saving state for rollback ...
```


Sample Output

request system software add (Mixed EX4200 and EX4500 Virtual Chassis)

```
user@switch> request system software add set
[/var/tmp/jinstall-ex-4200-11.1R1.1-domestic-signed.tgz
/var/tmp/jinstall-ex-4500-11.1R1.1-domestic-signed.tgz]
...
```

request system software add component all (QFabric Systems)

```
user@switch> request system software add /pbdata/packages/jinstall-qfabric-12.2X50-D1.3.rpm
component all
...
```

request system software add (Maintenance)

Syntax request system software add *package-name*

Release Information Partition option introduced in the command in Release 10.1. of Junos OS.

Description Installs the new software package on the device.

Options

- delay–restart — Installs the software package but does not restart the software process
- best-effort-load— Activate a partial load and treat parsing errors as warnings instead of errors
- no-copy — Installs the software package but does not saves the copies of package files
- no-validate— Does not check the compatibility with current configuration before installation starts
- partition — Formats and re-partitions the media before installation
- reboot— Reboots the device after installation is completed
- unlink—Removes the software package after successful installation
- validate—Checks the compatibility with current configuration before installation starts

Required Privilege Level maintenance

Example

user@host# request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot

request system software configuration-backup

Syntax request system software configuration-backup (*path*)

Release Information Command introduced in Junos OS Release 11.3 for the QFX Series.

Description Save the currently active configuration and any installation-specific parameters such as a configuration that you have entered outside of the CLI, Director group IP addresses, and the default partition IP address.

Options **path**—(QFabric System) Provide the path to the location of the backup configuration files. You can save the backup configuration files to either a URL, local directory, remote server, or removable drive.

Required Privilege Level configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.

Related Documentation

- request system software configuration-restore on page 384
- Performing a QFabric System Recovery Installation on the Director Group on page 229

List of Sample Output request system software configuration-backup on page 383

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software configuration-backup

```
user@switch request system software configuration-backup ftp://ftp.test.net/test
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                    Dload  Upload   Total   Spent    Left
Speed
100        4035     0     0    100 4035    0      138k --:--:-- --:--:-- --:--:--
  0
```

request system software configuration-restore

Syntax request system software configuration-restore (*path*)

Release Information Command introduced in Junos OS Release 11.3 for the QFX Series.

Description Restore a previously saved configuration and any installation-specific parameters, such as a configuration that you have entered outside of the CLI, Director group IP addresses, and the default partition IP address.

Options **path**—(QFabric System) Provide the path to the location of the backup configuration files. The path can be to a local file, a file on an external flash drive, or an SCP or FTP destination.

Required Privilege Level configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.

Related Documentation

- request system software configuration-backup on page 383
- Performing a QFabric System Recovery Installation on the Director Group on page 229

List of Sample Output request system software configuration-restore on page 384

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software configuration-restore

```
user@switch request system software configuration-restore ftp://ftp.test.net/test
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  4035  100  4035    0     0   153k      0 --:--:-- --:--:-- --:--:-- 3803k
```


request system software delete

List of Syntax

Syntax on page 385
Syntax (TX Matrix Router) on page 385
Syntax (TX Matrix Plus Router) on page 385

Syntax

request system software delete *software-package*
<force>
<reboot>
<set [*package-name package-name*]>

Syntax (TX Matrix Router)

request system software delete *software-package*
<force>
<lcc *number* | scc>
<reboot>
<set [*package-name package-name*]>

Syntax (TX Matrix Plus Router)

request system software delete *software-package*
<force>
<lcc *number* | sfc *number*>
<reboot>
<set [*package-name package-name*]>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Option **set [*package-name package-name*]** added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Services Gateways.
Option reboot introduced in Junos OS Release 12.3.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Remove a software package or bundle from the router or switch.

CAUTION: **Before removing a software package or bundle, make sure that you have already placed the new software package or bundle that you intend to load onto the router or switch.**

Options

software-package—Software package or bundle name. You can delete any or all of the following software bundles or packages:

- **jbase**—(Optional) Junos base software suite
- **jcrypto**—(Optional, in domestic version only) Junos security software
- **jdocs**—(Optional) Junos online documentation file
- **jkernel**—(Optional) Junos kernel software suite
- **jpfe**—(Optional) Junos Packet Forwarding Engine support

- **jroute**—(Optional) Junos routing software suite
- **junos**—(Optional) Junos base software

NOTE: On EX Series switches, some of the package names are different than those listed. To see the list of packages that you can delete on an EX Series switch, enter the command **show system software**.

force—(Optional) Ignore warnings and force removal of the software.

lcc ***number***—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, remove an extension or upgrade package from a specific T640 router (line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, remove an extension or upgrade package from a specific router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

reboot—As of Junos OS 12.3 and greater, automatically reboot upon completing the **request system software delete** command.

scc—(TX Matrix routers only) (Optional) Remove an extension or upgrade package from the TX Matrix router (or switch-card chassis).

set [*package-name package-name*]—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages or software add-on packages at the same time.

sfc ***number***—(TX Matrix Plus routers only) (Optional) Remove an extension or upgrade package from the TX Matrix Plus router. Replace *number* with 0.

Additional Information

Before upgrading the software on the router or switch, when you have a known stable system, issue the **request system snapshot** command to back up the software, including the configuration, to the /altroot and /altconfig file systems (on routers) or the /, /altroot, /config, /var, and /var/tmp file systems (on switches). After you have upgraded the software on the router or switch and are satisfied that the new packages are successfully installed and running, issue the **request system snapshot** command again to back up the new software to the /altroot and /altconfig file systems (on routers) or the /, /altroot,

/config, /var, and /var/tmp file systems (on switches). After you run the **request system snapshot** command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Required Privilege Level maintenance

Related Documentation

- request system software add on page 373
- request system software rollback on page 397
- request system software validate on page 402
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

List of Sample Output request system software delete jdocs on page 387

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software delete jdocs

The following example displays the system software packages before and after the **jdocs** package is deleted through the **request system software delete** command:

```
user@host> show system software
Information for jbase:

Comment:
JUNOS Base OS Software Suite [7.2R1.7]


Information for jcrypto:

Comment:
JUNOS Crypto Software Suite [7.2R1.7]


Information for jdocs:

Comment:
JUNOS Online Documentation [7.2R1.7]


Information for jkernel:

Comment:
JUNOS Kernel Software Suite [7.2R1.7]

...

user@host> request system software delete jdocs
Removing package 'jdocs' ...

user@host> show system software
```

```
Information for jbase:

Comment:
JUNOS Base OS Software Suite [7.2R1.7]


Information for jcrypto:

Comment:
JUNOS Crypto Software Suite [7.2R1.7]


Information for jkernel:

Comment:
JUNOS Kernel Software Suite [7.2R1.7]

...
```

request system software nonstop-upgrade

Syntax

request system software nonstop-upgrade *package-name*
<fabric >
<director-group>
<node-group *name*>

Release Information

Command introduced in Junos OS Release 12.2 for the QFX Series.

Description

Nonstop software upgrade enables you to upgrade a QFabric system with minimal packet loss and maximum uptime. You should upgrade the devices in the following order: Director group, fabric controls and Interconnect devices, and network and server Node groups.

NOTE: **Before you perform a nonstop software upgrade, contact JTAC to perform a pre-upgrade health check on the QFabric system.**

Options

package-name—Location from which the software is to be installed. For example:

- ***protocol://hostname/pathname/package-name***—For a software package or bundle that is to be downloaded and installed from a remote location. Replace ***protocol*** with one of the following:
  - **ftp**—File Transfer Protocol.
    Use **ftp*://hostname/pathname/package-name***. To specify authentication credentials, use
    ftp*://<username>:<password>@hostname/pathname/package-name*. To have the system prompt you for the password, specify **prompt** in place of the password. If a password is required, and you do not specify the password or **prompt**, an error message is displayed.
  - **http**—Hypertext Transfer Protocol.
    Use **http*://hostname/pathname/package-name***. To specify authentication credentials, use
    http*://<username>:<password>@hostname/pathname/package-name*. If a password is required and you omit it, you are prompted for it.
  - **scp**—Secure copy (available only for Canada and U.S. version).

Use **scp:*//hostname/pathname/package-name***. To specify authentication credentials, use **scp:*//<username>:<password>@hostname/pathname/package-name***.

NOTE:

- The ***pathname*** in the protocol is the relative path to the user's home directory on the remote system and not the root directory.

director-group—Install software package on the Director group and Fabric managers.

fabric—Install software package on the Interconnect devices and Fabric controls.

node-group *name* —Install software package on the redundant server Node group, server Node group, or network Node group.

Required Privilege Level maintenance

Related Documentation

- *Nonstop Software Upgrade Checklist for QFabric Systems*
- *Performing a Nonstop Software Upgrade on the QFabric System*
- Verifying Nonstop Software Upgrade for QFabric Systems on page 158
- show chassis nonstop-upgrade node-group on page 411

List of Sample Output

request system software nonstop-upgrade director-group on page 390
request system software nonstop-upgrade fabric on page 392
request system software nonstop-upgrade node-group (Redundant Server Node Group) on page 393
request system software nonstop-upgrade node-group (Server Node Group) on page 394

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software nonstop-upgrade director-group

```
user@qfabric> request system software nonstop-upgrade director-group
jinstall-qfabric-12.2X50-D10.3.rpm
Validating update package jinstall-qfabric-12.2X50-D10.3.rpm
Installing update package jinstall-qfabric-12.2X50-D10.3.rpm
Installing fabric images version 12.2X50-D10.3
Performing cleanup
Package install complete
Installing update package jinstall-qfabric-12.2X50-D10.3.rpm on peer
Triggering Initial Stage of Fabric Manager Upgrade
Updating CCIF default image to 12.2X50-D10.3
Updating FM-0 to Junos version 12.2X50-D10.3
[Status   2012-06-05 15:25:29]: Fabric Manager: Upgrade Initial Stage started
[FM-0     2012-06-05 15:25:38]: FM-0 Master already running on LOCAL DG
```



```
[NW-NG-0  2012-06-05 15:25:45]: NW-NG-0 Master already running on LOCAL DG
[FM-0     2012-06-05 15:26:12]: Retrieving package
[FM-0     2012-06-05 15:27:11]: Pushing bundle to re0
[Status   2012-06-05 15:29:06]: Load completed with 0 errors...
[Status   2012-06-05 15:29:06]: Reboot is required to complete upgrade ...
[Status   2012-06-05 15:29:07]: Trying to Connect to Node: FM-0
[Status   2012-06-05 15:29:13]: Rebooting FM-0
[FM-0     2012-06-05 15:29:13]: Waiting for FM-0 to terminate ...
Starting Peer upgrade

Initiating rolling upgrade of Director peer:  version 12.2X50-D10.3

Inform CCIF regarding rolling upgrade
[Peer Update Status]: Validating install package jinstall-qfabric-12.2X50-D10.3.rpm
[Peer Update Status]: Cleaning up node for rolling phase one upgrade
[Peer Update Status]: Director group upgrade complete
[Peer Update Status]: COMPLETED
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to reboot and start phase one of rolling
upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to return after reboot and start phase one
 of rolling upgrade
[Peer Update Status]: Waiting for peer to complete phase one of rolling upgrade
[Peer Update Status]: Peer completed phase one of rolling upgrade
Setting peer DG node as the master SFC

Delaying start of local upgrade to allow peer services time to initialize [15
minutes]
```

```
Delaying start of local upgrade to allow peer services time to initialize [15
minutes]
Delaying start of local upgrade to allow peer services time to initialize [12
minutes]
Delaying start of local upgrade to allow peer services time to initialize [9
minutes]
Delaying start of local upgrade to allow peer services time to initialize [6
minutes]
Delaying start of local upgrade to allow peer services time to initialize [3
minutes]
[Peer Update Status]: Check for VMs on dg0
Triggering Final Stage of Fabric Manager Upgrade:
Updating FM-0 to Junos version 12.2X50-D10.3
[Status   2012-06-05 16:10:12]: Fabric Manager: Upgrade Final Stage started
[NW-NG-0  2012-06-05 16:10:22]: Transferring NW-NG-0 Mastership to REMOTE DG
[NW-NG-0  2012-06-05 16:11:44]: Finished NW-NG-0 Mastership switch
[Status   2012-06-05 16:11:45]: Upgrading FM-0 VM on worker DG to 12.2X50-D10.3
[DRE-0    2012-06-05 16:12:43]: Retrieving package
[DRE-0    2012-06-05 16:13:46]: ------- re0: -------
[Status   2012-06-05 16:15:17]: Load completed with 0 errors...
[Status   2012-06-05 16:15:17]: Reboot is required to complete upgrade ...
[DRE-0    2012-06-05 16:15:22]: Waiting for DRE-0 to terminate ...
[DRE-0    2012-06-05 16:15:34]: Waiting for DRE-0 to come back ...
[DRE-0    2012-06-05 16:18:44]: Running Uptime Test for DRE-0
[DRE-0    2012-06-05 16:18:51]: Uptime Test for DRE-0 Passed ...
[Status   2012-06-05 16:18:51]: DRE-0 booted successfully ...
Performing post install shutdown and cleanup

Broadcast message from root (Tue Jun  5 16:18:51 2012):

The system is going down for reboot NOW!
Director group upgrade complete

root@qfabric> Read from remote host qfabric-partition0: Connection reset by peer
Connection to qfabric-partition0 closed.
```

request system software nonstop-upgrade fabric

```
user@qfabric> request system software nonstop-upgrade fabric
jinstall-qfabric-12.2X50-D10.3.rpm
[FC-0     2012-06-05 16:48:53]: Retrieving package
[FC-1     2012-06-05 16:48:53]: Retrieving package
[IC-F4912 2012-06-05 16:48:59]: Retrieving package
[FC-0     2012-06-05 16:49:51]: ------- re0: -------
[FC-1     2012-06-05 16:49:52]: ------- re0: -------
[IC-F4912 2012-06-05 16:49:54]: ------- re0: -------
[IC-F4912 2012-06-05 16:50:42]: Step 1 of 20 Creating temporary file system
[IC-F4912 2012-06-05 16:50:42]: Step 2 of 20 Determining installation source
[IC-F4912 2012-06-05 16:50:43]: Step 3 of 20 Processing format options
[IC-F4912 2012-06-05 16:50:43]: Step 4 of 20 Determining installation slice
[IC-F4912 2012-06-05 16:50:43]: Step 5 of 20 Creating and labeling new slices
[IC-F4912 2012-06-05 16:50:44]: Step 6 of 20 Create and mount new file system
[IC-F4912 2012-06-05 16:50:53]: Step 7 of 20 Getting OS bundles
[IC-F4912 2012-06-05 16:50:53]: Step 8 of 20 Updating recovery media
[IC-F4912 2012-06-05 16:51:17]: Step 9 of 20 Extracting incoming image
[IC-F4912 2012-06-05 16:52:56]: Step 10 of 20 Unpacking OS packages
[IC-F4912 2012-06-05 16:52:59]: Step 11 of 20 Mounting jbase package
[IC-F4912 2012-06-05 16:53:28]: Step 12 of 20 Creating base OS symbolic links
[IC-F4912 2012-06-05 16:54:45]: Step 13 of 20 Creating fstab
[IC-F4912 2012-06-05 16:54:45]: Step 14 of 20 Creating new system files
[IC-F4912 2012-06-05 16:54:46]: Step 15 of 20 Adding jbundle package
```

```
[IC-F4912 2012-06-05 16:58:15]: Step 16 of 20 Backing up system data
[IC-F4912 2012-06-05 16:58:18]: Step 17 of 20 Setting up shared partition data
[IC-F4912 2012-06-05 16:58:18]: Step 18 of 20 Checking package sanity in
installation
[IC-F4912 2012-06-05 16:58:18]: Step 19 of 20 Unmounting and cleaning up temporary
 file systems
[IC-F4912 2012-06-05 16:58:22]: Step 20 of 20 Setting da0s1 as new active partition
[Status   2012-06-05 16:58:34]: Load completed with 0 errors...
[Status   2012-06-05 16:58:34]: Reboot is required to complete upgrade ...
[Status   2012-06-05 16:58:34]: Trying to Connect to Node: FC-0
[Status   2012-06-05 16:58:39]: Rebooting FC-0
[Status   2012-06-05 16:58:39]: Trying to Connect to Node: FC-1
[Status   2012-06-05 16:58:44]: Rebooting FC-1
[Status   2012-06-05 16:58:44]: Trying to Connect to Node: IC-F4912
[Status   2012-06-05 16:58:50]: Rebooting IC-F4912
Success
```

request system software nonstop-upgrade node-group (Redundant Server Node Group)

```
user@qfabric> request system software nonstop-upgrade node-group RSNG
jinstall-qfabric-12.2X50-D10.3.rpm
Upgrading target(s): RSNG

[RSNG     2012-06-05 17:26:44]: Starting with package
ftp://169.254.0.3/pub/images/12.2X50-D10.3/jinstall-qfx.tgz
[RSNG     2012-06-05 17:26:44]: Retrieving package
[RSNG     2012-06-05 17:28:56]: Pushing bundle to fpc1
[RSNG     2012-06-05 17:29:26]: fpc1: Validate package...
[RSNG     2012-06-05 17:35:22]: fpc0: Validate package...
[RSNG     2012-06-05 17:35:49]: ------- fpc1 -------
[RSNG     2012-06-05 17:36:25]: Step 1 of 20 Creating temporary file system
[RSNG     2012-06-05 17:36:26]: Step 2 of 20 Determining installation source
[RSNG     2012-06-05 17:36:26]: Step 3 of 20 Processing format options
[RSNG     2012-06-05 17:36:26]: Step 4 of 20 Determining installation slice
[RSNG     2012-06-05 17:36:27]: Step 5 of 20 Creating and labeling new slices
[RSNG     2012-06-05 17:36:27]: Step 6 of 20 Create and mount new file system
[RSNG     2012-06-05 17:36:35]: Step 7 of 20 Getting OS bundles
[RSNG     2012-06-05 17:36:35]: Step 8 of 20 Updating recovery media
[RSNG     2012-06-05 17:36:56]: Step 9 of 20 Extracting incoming image
[RSNG     2012-06-05 17:38:07]: Step 10 of 20 Unpacking OS packages
[RSNG     2012-06-05 17:38:16]: Step 11 of 20 Mounting jbase package
[RSNG     2012-06-05 17:38:41]: Step 12 of 20 Creating base OS symbolic links
[RSNG     2012-06-05 17:39:41]: Step 13 of 20 Creating fstab
[RSNG     2012-06-05 17:39:42]: Step 14 of 20 Creating new system files
[RSNG     2012-06-05 17:39:42]: Step 15 of 20 Adding jbundle package
[RSNG     2012-06-05 17:42:16]: Step 16 of 20 Backing up system data
[RSNG     2012-06-05 17:42:32]: Step 17 of 20 Setting up shared partition data
[RSNG     2012-06-05 17:42:33]: Step 18 of 20 Checking package sanity in
installation
[RSNG    2012-06-05 17:42:33]: Step 19 of 20 Unmounting and cleaning up temporary
 file systems
[RSNG    2012-06-05 17:42:36]: Step 20 of 20 Setting da0s2 as new active partition
[RSNG     2012-06-05 17:42:51]: ------- fpc0 - master -------
[RSNG     2012-06-05 17:42:51]: Step 1 of 20 Creating temporary file system
[RSNG     2012-06-05 17:42:51]: Step 2 of 20 Determining installation source
[RSNG     2012-06-05 17:42:51]: Step 3 of 20 Processing format options
[RSNG     2012-06-05 17:42:51]: Step 4 of 20 Determining installation slice
[RSNG     2012-06-05 17:42:51]: Step 5 of 20 Creating and labeling new slices
[RSNG     2012-06-05 17:42:51]: Step 6 of 20 Create and mount new file system
[RSNG     2012-06-05 17:42:51]: Step 7 of 20 Getting OS bundles
[RSNG     2012-06-05 17:42:51]: Step 8 of 20 Updating recovery media
```

```
[RSNG     2012-06-05 17:42:51]: Step 9 of 20 Extracting incoming image
[RSNG     2012-06-05 17:42:51]: Step 10 of 20 Unpacking OS packages
[RSNG     2012-06-05 17:42:51]: Step 11 of 20 Mounting jbase package
[RSNG     2012-06-05 17:42:51]: Step 12 of 20 Creating base OS symbolic links
[RSNG     2012-06-05 17:42:51]: Step 13 of 20 Creating fstab
[RSNG     2012-06-05 17:42:51]: Step 14 of 20 Creating new system files
[RSNG     2012-06-05 17:42:51]: Step 15 of 20 Adding jbundle package
[RSNG     2012-06-05 17:42:51]: Step 16 of 20 Backing up system data
[RSNG     2012-06-05 17:42:51]: Step 17 of 20 Setting up shared partition data
[RSNG     2012-06-05 17:42:51]: Step 18 of 20 Checking package sanity in
installation
[RSNG    2012-06-05 17:42:51]: Step 19 of 20 Unmounting and cleaning up temporary
 file systems
[RSNG    2012-06-05 17:42:51]: Step 20 of 20 Setting da0s2 as new active partition
[RSNG     2012-06-05 17:43:36]: Rebooting Backup RE
[RSNG     2012-06-05 17:43:36]: ------- Rebooting fpc1 -------
[RSNG     2012-06-05 17:50:12]: Initiating Chassis In-Service-Upgrade
[RSNG     2012-06-05 17:50:33]: Upgrading group: 0 fpc: 0
[RSNG     2012-06-05 17:52:38]: Upgrade complete for group:0
[RSNG     2012-06-05 17:52:38]: Upgrading group: 1 fpc: 1
[RSNG     2012-06-05 17:54:42]: Upgrade complete for group:1
[RSNG    2012-06-05 17:54:42]: Finished processing all upgrade groups, last group
 :1
[RSNG     2012-06-05 17:54:48]: Preparing for Switchover
[RSNG     2012-06-05 17:55:38]: Switchover Completed
[Status   2012-06-05 17:55:41]: Upgrade completed with 0 errors
Success
```

request system software nonstop-upgrade node-group (Server Node Group)

```
user@qfabric> request system software nonstop-upgrade node-group P1507-C
jinstall-qfabric-12.2X50-D10.3.rpm
Upgrading target(s): P1507-C

[P1507-C  2012-06-26 14:02:44]: Retrieving package
[P1507-C  2012-06-26 14:03:21]: ------- P1507-C: -------
[P1507-C  2012-06-26 14:03:59]: Step 1 of 20 Creating temporary file system
[P1507-C  2012-06-26 14:03:59]: Step 2 of 20 Determining installation source
[P1507-C  2012-06-26 14:03:59]: Step 3 of 20 Processing format options
[P1507-C  2012-06-26 14:03:59]: Step 4 of 20 Determining installation slice
[P1507-C  2012-06-26 14:04:00]: Step 5 of 20 Creating and labeling new slices
[P1507-C  2012-06-26 14:04:00]: Step 6 of 20 Create and mount new file system
[P1507-C  2012-06-26 14:04:08]: Step 7 of 20 Getting OS bundles
[P1507-C  2012-06-26 14:04:09]: Step 8 of 20 Updating recovery media
[P1507-C  2012-06-26 14:04:29]: Step 9 of 20 Extracting incoming image
[P1507-C  2012-06-26 14:05:42]: Step 10 of 20 Unpacking OS packages
[P1507-C  2012-06-26 14:05:49]: Step 11 of 20 Mounting jbase package
[P1507-C  2012-06-26 14:06:14]: Step 12 of 20 Creating base OS symbolic links
[P1507-C  2012-06-26 14:07:15]: Step 13 of 20 Creating fstab
[P1507-C  2012-06-26 14:07:15]: Step 14 of 20 Creating new system files
[P1507-C  2012-06-26 14:07:16]: Step 15 of 20 Adding jbundle package
[P1507-C  2012-06-26 14:09:52]: Step 16 of 20 Backing up system data
[P1507-C  2012-06-26 14:10:07]: Step 17 of 20 Setting up shared partition data
[P1507-C  2012-06-26 14:10:07]: Step 18 of 20 Checking package sanity in
installation
[P1507-C  2012-06-26 14:10:08]: Step 19 of 20 Unmounting and cleaning up temporary
 file systems
[P1507-C  2012-06-26 14:10:11]: Step 20 of 20 Setting da0s2 as new active partition
[Status   2012-06-26 14:10:25]: Trying to Connect to Node: P1507-C
[Status   2012-06-26 14:10:32]: Rebooting P1507-C
```

```
[Status   2012-06-26 14:10:32]: Upgrade completed with 0 errors
Success
```

request system software reboot

Syntax request system software reboot *<at time> <in minutes><media><message 'text">*

Release Information Command introduced in Release 10.1 of Junos OS.

Description Reboots the software.

Options

- at time— Specifies the time at which to reboot the device . You can specify time in one of the following ways:
  - now— Reboots the device immediately. This is the default.
  - +minutes— Reboots the device in the number of minutes from now that you specify.
  - yymmddhhmm— Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.
  - hh:mm— Reboots the device at the absolute time you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
- in minutes — Specifies the number of minutes from now to reboot the device. This option is a synonym for the at +minutes option
- media type— Specifies the boot device to boot the device from:
  - internal— Reboots from the internal media. This is the default.
  - usb— Reboots from the USB storage device.
  - external— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.
- message "text"— Provides a message to display to all system users before the device reboots.

  Example: **request system reboot at 5 in 50 media internal message stop**

Required Privilege Level maintenance

Related Documentation

- *Device Configuration*

request system software rollback

List of Syntax

Syntax

request system software rollback

Syntax (EX Series Switches)

request system software rollback
<all-members>
<local>
<member *member-id*>
<reboot>

Syntax (TX Matrix Router)

request system software rollback
<lcc *number* | scc>
<reboot>

Syntax (TX Matrix Plus Router)

request system software rollback
<lcc *number* | sfc *number*>
<reboot>

Syntax (MX Series Router)

request system software rollback
<all-members>
<local>
<member *member-id*>
<reboot>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command behavior changed in Junos OS Release 12.1.
Option **reboot** introduced in Junos OS Release 12.3.

Description

For all versions of Junos OS up to and including Junos OS 11.4, revert to the software that was loaded at the last successful **request system software add** command.

As of Junos OS 12.1 and greater, revert to the last known good state before the most recent **request system software (add | delete)** command. For example, using rollback in Junos OS 12.1 after using **request system software add** restores the system to a known good state prior to using the **add** command. Similarly, using rollback in Junos OS 12.1 after using **request system software delete** restores the system to a known good state prior to using the **delete** command.

A software rollback fails if any required package (or a **jbundle** package containing the required package) cannot be found in /var/sw/pkg.

Additional Information

- On M Series and T Series routers, if **request system software add <jinstall> reboot** was used for the previous installation, then **request system software rollback** has no effect. In this case, use **jinstall** to reinstall the required package.
- On M Series and T Series routers, if **request system software add <sdk1>** was used for the previous installation, then **request system software rollback** removes the last installed SDK package (**sdk1** in this example).
- On SRX Series devices with dual root systems, when **request system software rollback** is run, the system switches to the alternate root. Each root can have a different version of Junos OS. Rollback takes each root back to the previously installed image.
- On QFX3500 and QFX3600 devices in a mixed Virtual Chassis, when the **request system software rollback** command is issued, the system does not rollback to the image stored in the alternate partition.
- On QFX5100 switches, the **reboot** option has been removed. To reboot the switch after a software rollback, issue the **request system reboot** command as a separate, secondary command.

Options

all-members—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on all members of the Virtual Chassis configuration.

lcc ***number***—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, attempt to roll back to the previous set of packages on a T640 router connected to the TX Matrix router. On a TX Matrix Plus router, attempt to roll back to the previous set of packages on a connected router connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on the local Virtual Chassis member.

member ***member-id***—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace ***member-id*** with a value from 0 through 9. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

none—For all versions of Junos OS up to and including Junos OS 11.4, revert to the set of software as of the last successful **request system software add**. As of Junos OS 12.1 and greater, revert to the last known good state before the most recent **request system software (add | delete)** command.

reboot—As of Junos OS 12.3 and greater, automatically reboot upon completing the **request system software rollback** command.

scc—(TX Matrix routers only) (Optional) Attempt to roll back to the previous set of packages on the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Attempt to roll back to the previous set of packages on the TX Matrix Plus router. Replace *number* with 0.

Required Privilege Level

maintenance

Related Documentation

- *request system software abort*
- request system software add on page 373
- request system software delete on page 385
- request system software validate on page 402
- *request system configuration rescue delete*
- *request system configuration rescue save*
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

List of Sample Output

request system software rollback on page 400

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software rollback

```
user@host> request system software rollback
Verified SHA1 checksum of ./jbase-7.2R1.7.tgz
Verified SHA1 checksum of ./jdocs-7.2R1.7.tgz
Verified SHA1 checksum of ./jroute-7.2R1.7.tgz
Installing package './jbase-7.2R1.7.tgz' ...
Available space: 35495 require: 7335
Installing package './jdocs-7.2R1.7.tgz' ...
Available space: 35339 require: 3497
Installing package './jroute-7.2R1.7.tgz' ...
Available space: 35238 require: 6976
NOTICE: uncommitted changes have been saved in
/var/db/config/juniper.conf.pre-install
Reloading /config/juniper.conf.gz ...
Activating /config/juniper.conf.gz ...
mgd: commit complete
Restarting mgd ...
Restarting aprobed ...
Restarting apsd ...
Restarting cosd ...
Restarting fsad ...
Restarting fud ...
Restarting gcdrd ...
Restarting ilmid ...
Restarting irsd ...
Restarting l2tpd ...
Restarting mib2d ...
Restarting nasd ...
Restarting pppoed ...
Restarting rdd ...
Restarting rmopd ...
Restarting rtspd ...
Restarting sampled ...
Restarting serviced ...
Restarting snmpd ...
Restarting spd ...
Restarting vrrpd ...

WARNING: cli has been replaced by an updated version:
CLI release 7.2R1.7 built by builder on 2005-04-22 02:03:44 UTC
Restart cli using the new version ? [yes,no] (yes) yes

Restarting cli ...
user@host
```

request system software rollback (Maintenance)

Syntax request system software rollback

Release Information Command introduced in Release 10.1 of Junos OS.

Description Revert to the software that was loaded at the last successful **request system software add** command. Example: **request system software rollback**

Required Privilege Level maintenance

Example

```
user@host# request system software rollback
```

request system software validate

List of Syntax

Syntax on page 402
Syntax (TX Matrix Router) on page 402
Syntax (TX Matrix Plus Router) on page 402
Syntax (MX Series Router) on page 402

Syntax

request system software validate *package-name*
<set [*package-name package-name*]>
<upgrade-with-config>
<upgrade-with-config-format *format*>

Syntax (TX Matrix Router)

request system software validate *package-name*
<lcc *number* | scc>
<set [*package-name package-name*]>
<upgrade-with-config>
<upgrade-with-config-format *format*>

Syntax (TX Matrix Plus Router)

request system software validate *package-name*
<lcc *number* | sfc *number*>
<set [*package-name package-name*]>
<upgrade-with-config>
<upgrade-with-config-format *format*>

Syntax (MX Series Router)

request system software validate *package-name*
<member *member-id*>
<set [*package-name package-name*]>
<upgrade-with-config>
<upgrade-with-config-format *format*>

Release Information

Command introduced before Junos OS Release 7.4.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
set [*package-name package-name*] option added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways.
upgrade-with-config and **upgrade-with-config-format *format*** options added in Junos OS Release 12.3 for M Series routers, MX Series routers, and T Series routers.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Validate candidate software against the current configuration of the router.

Options

lcc *number*—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, validate the software bundle or package on a specific T640 router (or line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, validate the software bundle or package for a specific router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

member ***member-id***—(MX Series routers only) (Optional) Validate the software bundle or package on the specified member of the Virtual Chassis configuration. For an MX Series Virtual Chassis, replace ***member-id*** with a value of 0 or 1.

package-name—Name of the software bundle or package to test.

scc—(TX Matrix routers only) (Optional) Validate the software bundle or package for the TX Matrix router (or switch-card chassis).

set [*package-name package-name*]—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages or software add-on packages at the same time.

sfc ***number***—(TX Matrix Plus routers only) (Optional) Validate the software bundle or package for the TX Matrix Plus router.

upgrade-with-config—(Optional) Install one or more configuration files.

upgrade-with-config-format ***format***—(Optional) Specify the configuration file fomat, **text** or **xml**. The default format is **text**.

NOTE: The **upgrade-with-config** and **upgrade-with-config-format** options are only available locally on the router or switch. In a routing matrix, the configuration is applied only to the local router and is not propagated to other routers.

The options are validated during the validation process and applied to the router or switch during the upgrade process. If the upgrade process is successful, the options are removed from the configuration. If the upgrade process fails, the configuration file is renamed with the .failed suffix.

Additional Information

By default, when you issue the **request system software validate** command on a TX Matrix master Routing Engine, all the T640 master Routing Engines that are connected to it are validated. If you issue the same command on the TX Matrix backup Routing Engine, all

the T640 backup Routing Engines that are connected to it are upgraded to the same version of software.

Likewise, if you issue the **request system software validate** command on a TX Matrix Plus master Routing Engine, all the T1600 or T4000 master Routing Engines that are connected to it are validated. If you issue the same command on a TX Matrix Plus backup Routing Engine, all the T1600 or T4000 backup Routing Engines that are connected to it are upgraded to the same version of software.

Required Privilege Level maintenance

Related Documentation

- *request system software abort*
- request system software add on page 373
- request system software delete on page 385
- request system software rollback on page 397
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

List of Sample Output

request system software validate (Successful Case) on page 404
request system software validate (Failure Case) on page 404

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software validate (Successful Case)

```
user@host> request system software validate /var/sw/pkg/jbundle-5.3I20020124_0520_sjg.tgz
Checking compatibility with configuration
Initializing...
Using /packages/jbase-5.3I20020122_1901_sjg
Using /var/sw/pkg/jbundle-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jbase-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jkernel-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jcrypto-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jpfe-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jdocs-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jroute-5.3I20020124_0520_sjg.tgz
Validating against /config/juniper.conf.gz
mgd: commit complete

WARNING: cli has been replaced by an updated version:
CLI release 5.3I0 built by sjg on 2002-01-24 05:23:53 UTC
Restart cli using the new version ? [yes,no] (yes)
```

request system software validate (Failure Case)

```
user@host> request system software validate 6.3/
Pushing bundle to lcc0-re0
error: Failed to transfer package to lcc0-re0


user@host> request system software validate test
```



```
Pushing bundle to lcc0-re0
Pushing bundle to lcc2-re0

lcc0-re0:
gzip: stdin: not in gzip format
tar: child returned status 1
ERROR: Not a valid package: /var/tmp/test
```

request system zeroize

Syntax

request system zeroize
<media>
<local>

Release Information

Command introduced before Junos OS Release 9.0.
Command introduced in Junos OS Release 11.2 for EX Series switches.
Option **media** added in Junos OS Release 11.4 for EX Series switches.
Command introduced in Junos OS Release 12.2 for MX Series routers.
Command introduced in Junos OS Release 12.3 for the QFX Series.
Option **local** added in Junos OS Release 14.1.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

NOTE: **The media option is not available on the QFX Series.**

Remove all configuration information on the Routing Engines and reset all key values. If the device has dual Routing Engines, the command is broadcast to all Routing Engines on the device. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories. The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as **root** and start the Junos OS CLI by typing **cli** at the prompt.

NOTE: **If you configure the commit synchronize statement at the [edit system] hierarchy level and issue a commit in the master Routing Engine, the master configuration is automatically synchronized with the backup. However, if the backup Routing Engine is down when you issue the commit, the Junos OS displays a warning and commits the candidate configuration in the master Routing Engine. When the backup Routing Engine comes up, its configuration will automatically be synchronized with the master. A newly inserted backup Routing Engine automatically synchronizes its configuration with the master Routing Engine configuration.**

To completely erase user-created data so that it is unrecoverable, use the **media** option.

Options

media—(Optional) In addition to removing all configuration and log files, causes memory and the media to be scrubbed, removing all traces of any user-created files. Every storage device attached to the system is scrubbed, including disks, flash drives, removable USBs, and so on. The duration of the scrubbing process is dependent on the size of the media being erased. As a result, the **request system zeroize media**

operation can take considerably more time than the **request system zeroize** operation. However, the critical security parameters are all removed at the beginning of the process.

local—(Optional) Remove all the configuration information and restore all the key values on the active Routing Engine.

Required Privilege Level maintenance

Related Documentation

- request system snapshot on page 365
- *request system snapshot*
- *Reverting to the Default Factory Configuration for the EX Series Switch*
- *Reverting to the Rescue Configuration for the EX Series Switch*
- Reverting to the Default Factory Configuration on page 248
- Reverting to the Rescue Configuration on page 249
- Reverting to the Default Factory Configuration by Using the request system zeroize Command on page 248

List of Sample Output

Sample Output

request system zeroize

```
user@host> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes

0 1 1 0 0 0 done

syncing disks... All buffers synced.
Uptime: 5d19h20m26s
recorded reboot as normal shutdown
Rebooting...

U-Boot 1.1.6 (Mar 11 2011 - 04:39:06)

Board: EX4200-24T 2.11
EPLD:  Version 6.0 (0x85)
DRAM:  Initializing (1024 MB)
FLASH: 8 MB

Firmware Version: --- 01.00.00 ---
USB:   scanning bus for devices... 2 USB Device(s) found
       scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.4
(user@juniper.net, Fri Mar 11 03:03:36 UTC 2011)
```

```
Memory: 1024MB
bootsequencing is enabled
bootsuccess is set
new boot device = disk0s1:
Loading /boot/defaults/loader.conf
/kernel data=0x915c84+0xa1260 syms=[0x4+0x7cbd0+0x4+0xb1c19]


Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
JUNOS 11.1R1.8 #0: 2011-03-09 20:14:25 UTC

user@juniper.net:/volume/build/junos/11.1/release/11.1R1.8/obj-powerpc/bsd/kernels/
  JUNIPER-EX/kernel
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HID0 80004080
...
```

request system zeroize media

```
user@host> request system zeroize media
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes

warning: ipsec-key-management subsystem not running - not needed by configuration.
warning: zeroizing fpc0

{master:0}
root> Waiting (max 60 seconds) for system process `vnlru' to stop...done
. . .
Syncing disks, vnodes remaining...2 4 2 4 3 2 1 1 0 0 0 done

syncing disks... All buffers synced.
Uptime: 14m50s
recorded reboot as normal shutdown
Rebooting...

U-Boot 1.1.6 (Apr 21 2011 - 13:58:42)

Board: EX4200-48PX 1.1
EPLD:  Version 8.0 (0x82)
DRAM:  Initializing (512 MB)
FLASH: 8 MB
NAND:  No NAND device found!!!
0 MiB

Firmware Version: --- 01.00.00 ---
USB:   scanning bus for devices... 2 USB Device(s) found
       scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
```



```
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.2
(vtseng@svl-junos-pool27.juniper.net, Fri Feb 26 17:48:51 PST 2010)
Memory: 512MB
Loading /boot/defaults/loader.conf
/kernel data=0x9abfdc+0xb06e4 syms=[0x4+0x83b30+0x4+0xbd7c6]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel] in 1 second... Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
 The Regents of the University of California. All rights reserved.
JUNOS 11.4R1.2 #0: 2011-10-27 18:05:39 UTC
    user@juniper.net:/volume/build/junos/11.4/release/11.4R1.2/obj-powerpc/
bsd/kernels/JUNIPER-EX/kernel
can't re-use a leaf (all_slot_serialid)!
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HID0 80004080<EMCP,TBEN,EN_MAS7_UPDATE>
real memory  = 511705088 (488 MB)
avail memory = 500260864 (477 MB)
ETHERNET SOCKET BRIDGE initialising
Initializing EXSERIES platform properties ...
. . .
Automatic reboot in progress...
Media check on da0 on ex platforms
** /dev/da0s2a
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 20055 free (31 frags, 2503 blocks, 0.0% fragmentation)
zeroizing /dev/da0s1a ...
. . .
zeroizing /dev/da0s3d ...
. . .
zeroizing /dev/da0s3e ...
. . .
zeroizing /dev/da0s4d ...
. . .
zeroizing /dev/da0s4e ...
. . .

syncing disks... All buffers synced.
Uptime: 3m40s
Rebooting...

U-Boot 1.1.6 (Apr 21 2011 - 13:58:42)

Board: EX4200-48PX 1.1
EPLD:  Version 8.0 (0x82)
DRAM:  Initializing (512 MB)
FLASH: 8 MB
NAND:  No NAND device found!!!
0 MiB

Firmware Version: --- 01.00.00 ---
```

```
USB:   scanning bus for devices... 2 USB Device(s) found
       scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.2
(vtseng@svl-junos-pool27.juniper.net, Fri Feb 26 17:48:51 PST 2010)
Memory: 512MB
Loading /boot/defaults/loader.conf
/kernel data=0x9abfdc+0xb06e4 syms=[0x4+0x83b30+0x4+0xbd7c6]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel] in 1 second... Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
 The Regents of the University of California. All rights reserved.
JUNOS 11.4R1.2 #0: 2011-10-27 18:05:39 UTC
    user@juniper.net:/volume/build/junos/11.4/release/11.4R1.2/obj-powerpc/
bsd/kernels/JUNIPER-EX/kernel
can't re-use a leaf (all_slot_serialid)!
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HID0 80004080 <EMCP,TBEN,EN_MAS7_UPDATE>
real memory  = 511705088 (488 MB)
avail memory = 500260864 (477 MB)
ETHERNET SOCKET BRIDGE initialising
Initializing EXSERIES platform properties ...
. . .
Automatic reboot in progress...
Media check on da0 on ex platforms
** /dev/da0s1a
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 20064 free (48 frags, 2502 blocks, 0.1% fragmentation)
zeroizing /dev/da0s2a ...
. . .
Creating initial configuration...mgd: error: Cannot open configuration file:
/config/juniper.conf
mgd: warning: activating factory configuration
mgd: commit complete
mgd: ------------------------------------------------------------
mgd: Please login as 'root'. No password is required.
mgd: To start Initial Setup, type 'ezsetup' at the JUNOS prompt.
mgd: To start JUNOS CLI, type 'cli' at the JUNOS prompt.
mgd: ------------------------------------------------------------
Setting initial options:  debugger_on_panic=NO debugger_on_break=NO.
Starting optional daemons: .
Doing initial network setup:
. . .

Amnesiac (ttyu0)
```


show chassis nonstop-upgrade node-group

Syntax **show chassis nonstop-upgrade node-group** ***node-group-name***

Release Information Command introduced in Junos OS Release 12.2 for the QFX Series.

Description Display the status of the Node group after the most recent nonstop software upgrade (NSSU).

Required Privilege Level view

Related Documentation

- *Performing a Nonstop Software Upgrade on the QFabric System*
- request system software nonstop-upgrade on page 389

List of Sample Output show chassis nonstop-upgrade node-group on page 411

Output Fields Table 37 on page 411 lists the output fields for the **show chassis nonstop-upgrade node-group** command. Output fields are listed in the approximate order in which they appear.

Table 37: show chassis nonstop-upgrade node-group Output Fields

Field Name	Field Description
Item	Node device slot number.
Status	State of Node device: • **Error**—Node device is in an error state. • **Offline**—Node device is powered down. • **Online**—Node device is online and running.
Reason	Reason for the state (if the line card is offline).

Sample Output

show chassis nonstop-upgrade node-group

```
user@qfabric> show chassis nonstop-upgrade node-group NW-NG-0
 Item            Status                    Reason
  P1550-C         Online
```

show chassis usb storage

Syntax show chassis usb storage

Release Information Command introduced in Junos OS Release 11.4 R2.

Description Displays the current status of any USB mass storage device and whether the USB ports are enabled or disabled.

Required Privilege Level view

Related Documentation
- *Installation and Upgrade Guide*

List of Sample Output
show chassis hardware detail on page 412
show chassis usb storage on page 412

Sample Output

show chassis hardware detail

```
user@host> show chassis hardware detail
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                BV4911AA0005      SRX240H2-POE
Routing Engine   REV 01   750-043613   AAEC1923          RE-SRX240H2-POE
  usb0 (addr 1)  DWC OTG root hub 0    vendor 0x0000     uhub0
  usb0 (addr 2)  product 0x005a 90     vendor 0x0409     uhub1
  usb0 (addr 3)  ST72682  High Speed Mode 64218 STMicroelectronics umass0
  usb0 (addr 4)  Mass Storage Device 4096 JetFlash       umass1
FPC 0                                                    FPC
  PIC 0                                                  16x GE Base PIC
Power Supply 0
```

show chassis usb storage

```
user@host> show chassis usb storage
USB Disabled
```

show system auto-snapshot

Syntax **show system auto-snapshot**

Release Information Command introduced in Junos OS Release 12.3 for EX Series switches.
Command introduced in Junos OS Release 12.1X45-D10 for SRX Series devices.

Description Display automatic snapshot status information. When the automatic snapshot feature is enabled and the system reboots from the alternate root partition, the switch automatically takes a snapshot of the root file system in the alternate root partition and copies it onto the primary root partition. This automatic snapshot procedure takes place whenever the system reboots from the alternate partition, regardless of whether the reboot from the alternate partition is due to a command or due to a corruption of the primary partition.

When the automatic snapshot procedure is in progress, you cannot run the manual snapshot command, **request system snapshot**.

Options This command has no options.

Required Privilege Level view

Related Documentation
- Understanding Resilient Dual-Root Partitions on Switches on page 93

List of Sample Output **show system auto-snapshot on page 414**

Output Fields Table 38 on page 413 describes the output fields for the **show system auto-snapshot** command. Output fields are listed in the approximate order in which they appear.

Table 38: show system auto-snapshot status Output Fields

Field Name	Field Description
Auto-snapshot configuration	Status of the configuration: • Enabled—If the system reboots from the alternate partition, the automatic snapshot feature automatically takes a snapshot of the alternate partition and copies it onto the primary partition. • Disabled—The system does not automatically take a snapshot of the alternate partition. You must use the manual snapshot command, **request system snapshot**, to take a snapshot of one partition and copy it onto the other.
Auto-snapshot state	Status of the automatic snapshot procedure: • **Completed**—The automatic snapshot procedure has completed copying the alternate partition to the primary partition and the alarm has been cleared. • **Disabled**—The automatic snapshot procedure is inactive. • **In progress**—The automatic snapshot procedure is in progress. It takes about 10 to 15 minutes to complete, depending upon disk size.

Sample Output

show system auto-snapshot

```
user@switch> show system auto-snapshot
Auto-snapshot Configuration: Enabled
Auto-snapshot State: Disabled
```

show system autoinstallation status

Syntax show system autoinstallation status

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command supported in Junos OS Release 12.2 for ACX Series Universal Access Routers.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (ACX Series routers, J Series routers, and EX Series switches, QFX Series, and OCX Series only) Display autoinstallation status information.

Options This command has no options.

Required Privilege Level view

Related Documentation

- *ACX Series Autoinstallation Overview*
- *Before You Begin Autoinstallation on an ACX Series Universal Access Router*
- *Autoinstallation Configuration of ACX Series Universal Access Routers*
- *USB Autoinstallation on ACX Series Routers*
- *Autoinstalling a Configuration File from a Disk-on-Key USB Memory Stick onto an EX2200 or EX3300 Switch*
- *Verifying Autoinstallation on ACX Series Universal Access Routers*
- *autoinstallation*

List of Sample Output show system autoinstallation status on page 416

Output Fields Table 39 on page 415 describes the output fields for the **show system autoinstallation status** command. Output fields are listed in the approximate order in which they appear.

Table 39: show system autoinstallation status Output Fields

Field Name	Field Description

Autoinstallation status	Display autoinstallation status information:
	• **Last committed file**—File last committed for autoinstallation configuration.
	• **Configuration server of last committed file**—IP address or URL of the server configured to retrieve configuration information for the last committed configuration file.
	• **Interface**—Interface configured for autoinstallation.
	  ◦ **Name**—Name of the interface.
	  ◦ **State**—Interface state.
	• **Address acquisition**—Display IP address acquired and protocol used for acquisition upon startup.
	  ◦ **Protocol**—Protocol used for acquisition: BOOTP/DHCP or RARP.
	  ◦ **Acquired address**—IP address acquired from the DHCP server.

Sample Output

show system autoinstallation status

```
user@host> show system autoinstallation status
Autoinstallation status:
Master state: Active
Last committed file: None
Configuration server of last committed file: 0.0.0.0
Interface:
  Name: ge-0/0/1
  State: None
  Address acquisition:
    Protocol: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
```

show system autorecovery state

Syntax show system autorecovery state

Release Information Command introduced in Release 11.2 of Junos OS.

Description Performs checks and shows status of all autorecovered items.

Required Privilege Level view

Related Documentation
- request system autorecovery state on page 342
- *Installation and Upgrade Guide*

List of Sample Output show system autorecovery state on page 417

Output Fields Table 40 on page 417 lists the output fields for the **show system autorecovery state** command. Output fields are listed in the approximate order in which they appear.

Table 40: show system autorecovery state Output Fields

Field Name	Field Description
File	The name of the file on which autorecovery checks are performed.
Slice	The disk partition on which autorecovery checks are performed.
Recovery Information	Indicates whether autorecovery information for the file or slice has been saved.
Integrity Check	Displays the status of the file's integrity check (passed or failed).
Action / Status	Displays the status of the item, or the action required to be taken for that item.

Sample Output

show system autorecovery state

```
user@host> show system autorecovery state

Configuration:
File            Recovery Information    Integrity Check    Action / Status
rescue.conf.gz  Saved                   Passed             None
Licenses:
File            Recovery Information    Integrity Check    Action / Status
JUNOS282736.lic Saved                   Passed             None
JUNOS282737.lic Not Saved               Not checked        Requires save
BSD Labels:
Slice           Recovery Information    Integrity Check    Action / Status
s1              Saved                   Passed             None
s2              Saved                   Passed             None
s3              Saved                   Passed             None
s4              Saved                   Passed             None
```

show system boot-messages

List of Syntax

Syntax on page 419
Syntax (EX Series Switches) on page 419
Syntax (TX Matrix Router) on page 419
Syntax (TX Matrix Plus Router) on page 419
Syntax (MX Series Router) on page 419
Syntax (QFX Series) on page 419

Syntax

show system boot-messages

Syntax (EX Series Switches)

show system boot-messages
<all-members>
<local>
<member *member-id*>

Syntax (TX Matrix Router)

show system boot-messages
<all-chassis | all-lcc | lcc *number* | scc>

Syntax (TX Matrix Plus Router)

show system boot-messages
<all-chassis | all-lcc | lcc *number* | sfc *number*>

Syntax (MX Series Router)

show system boot-messages
<all-members>
<local>
<member *member-id*>

Syntax (QFX Series)

show system boot-messages
infrastructure *name* | interconnect-device *name* | node-group *name*

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display initial messages generated by the system kernel upon startup. These messages are the contents of **/var/run/dmesg.boot**.

Options

none—Display all boot time messages.

all-chassis—(TX Matrix routers andTX Matrix Plus routers only) (Optional) Display boot time messages for all of the chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display boot time messages for all T640 routers connected to a TX Matrix router. On a TX Matrix Plus router, display boot time messages for all connected T1600 or T4000 LCCs.

all-members—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on all members of the Virtual Chassis configuration.

infrastructure ***name***—(QFabric systems only) (Optional) Display boot time messages on the fabric control Routing Engine or fabric manager Routing engines.

interconnect-device ***name***—(QFabric systems only) (Optional) Display boot time messages on the Interconnect device.

lcc ***number***—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display boot time messages for a specific T640 router connected to a TX Matrix router. On a TX Matrix Plus router, display boot time messages for a specific router connected to a TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on the local Virtual Chassis member.

member ***member-id***—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace ***member-id*** with a value from 0 through 9. For an MX Series Virtual Chassis, replace ***member-id*** with a value of 0 or 1.

node-group ***name***—(QFabric systems only) (Optional) Display boot time messages on the Node group.

scc—(TX Matrix routers only) (Optional) Display boot time messages for the TX Matrix router (or switch-card chassis).

sfc ***number***—(TX Matrix Plus routers only) (Optional) Display boot time messages for the TX Matrix Plus router. Replace *number* with **0**.

Additional Information

By default, when you issue the **show system boot-messages** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level

view

Related Documentation

- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

List of Sample Output

Sample Output

show system boot-messages (TX Matrix Router)

```
user@host> show system boot-messages
Copyright (c) 1992-1998 FreeBSD Inc.
Copyright (c) 1996-2000 Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
        The Regents of the University of California.  All rights reserved.

JUNOS 4.1-20000216-Zf8469 #0: 2000-02-16 12:57:28 UTC
    tlim@single.juniper.net:/p/build/20000216-0905/4.1/release_kernel/sys/compil
e/GENERIC
CPU: Pentium Pro (332.55-MHz 686-class CPU)
  Origin = "GenuineIntel"  Id = 0x66a  Stepping=10
  Features=0x183f9ff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,SEP,MTRR,PGE,MCA,CMOV,<b
16>,<b17>,MMX,<b24>>
Teknor CPU Card Recognized
real memory  = 805306368 (786432K bytes)
avail memory = 786280448 (767852K bytes)
Probing for devices on PCI bus 0:
chip0 <generic PCI bridge (vendor=8086 device=7192 subclass=0)> rev 3 class 6000
0 on pci0:0:0
chip1 <Intel 82371AB PCI-ISA bridge> rev 1 class 60100 on pci0:7:0
chip2 <Intel 82371AB IDE interface> rev 1 class 10180 on pci0:7:1
chip3 <Intel 82371AB USB interface> rev 1 class c0300 int d irq 11 on pci0:7:2
smb0 <Intel 82371AB SMB controller> rev 1 class 68000 on pci0:7:3
pcic0 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int a irq 15 on pci0:13
:0
TI1131 PCI Config Reg: [pci only][FUNC0 pci int]
pcic1 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int b irq 12 on pci0:13
:1
TI1131 PCI Config Reg: [pci only][FUNC1 pci int]
fxp0 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 12 on

 pci0:16:0
chip4 <generic PCI bridge (vendor=1011 device=0022 subclass=4)> rev 4 class 6040
0 on pci0:17:0
fxp1 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on

 pci0:19:0
Probing for devices on PCI bus 1:
mcs0 <Miscellaneous Control Subsystem> rev 12 class ff0000 int a irq 12 on pci1:
13:0
fxp2 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on

 pci1:14:0
Probing for devices on the ISA bus:
sc0 at 0x60-0x6f irq 1 on motherboard
sc0: EGA color <16 virtual consoles, flags=0x0>
ed0 not found at 0x300
```

```
ed1 not found at 0x280
ed2 not found at 0x340
psm0 not found at 0x60
sio0 at 0x3f8-0x3ff irq 4 flags 0x20010 on isa
sio0: type 16550A, console
sio1 at 0x3e8-0x3ef irq 5 flags 0x20000 on isa
sio1: type 16550A
sio2 at 0x2f8-0x2ff irq 3 flags 0x20000 on isa
sio2: type 16550A
pcic0 at 0x3e0-0x3e1 on isa
PC-Card ctlr(0) TI PCI-1131 [CardBus bridge mode] (5 mem & 2 I/O windows)
pcic0: slot 0 controller I/O address 0x3e0
npx0 flags 0x1 on motherboard
npx0: INT 16 interface
fdc0: direction bit not set
fdc0: cmd 3 failed at out byte 1 of 3
fdc0 not found at 0x3f0
wdc0 at 0x1f0-0x1f7 irq 14 on isa
wdc0: unit 0 (wd0): <SunDisk SQFXB-80>, single-sector-i/o
wd0: 76MB (156672 sectors), 612 cyls, 8 heads, 32 S/T, 512 B/S
wdc0: unit 1 (wd1): <IBM-DCXA-210000>
wd1: 8063MB (16514064 sectors), 16383 cyls, 16 heads, 63 S/T, 512 B/S
wdc1 not found at 0x170
wdc2 not found at 0x180
ep0 not found at 0x300
fxp0: Ethernet address 00:a0:a5:12:05:5a
fxp1: Ethernet address 00:a0:a5:12:05:59
fxp2: Ethernet address 02:00:00:00:00:01
swapon: adding /dev/wd1s1b as swap device
Automatic reboot in progress...
/dev/rwd0s1a: clean, 16599 free (95 frags, 2063 blocks, 0.1% fragmentation)
/dev/rwd0s1e: clean, 9233 free (9 frags, 1153 blocks, 0.1% fragmentation)
/dev/rwd0s1a: clean, 16599 free (95 frags, 2063 blocks, 0.1% fragmentation)
/dev/rwd1s1f: clean, 4301055 free (335 frags, 537590 blocks, 0.0% fragmentation)
```

show system boot-messages lcc (TX Matrix Router)

```
user@host> show system boot-messages lcc 2
lcc2-re0:
--------------------------------------------------------------------------
Copyright (c) 1996-2001, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2001 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
JUNOS 7.0-20040912.0 #0: 2004-09-12 09:16:32 UTC

builder@benten.juniper.net:/build/benten-b/7.0/20040912.0/obj-i386/sys/compile/JUNIPER
Timecounter "i8254"  frequency 1193182 Hz
Timecounter "TSC"  frequency 601368936 Hz
CPU: Pentium III/Pentium III Xeon/Celeron (601.37-MHz 686-class CPU)
  Origin = "GenuineIntel"  Id = 0x68a  Stepping = 10

Features=0x387f9ff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,SEP,MTRR,PGE,MCA,CMOV,PAT,PSE36,PN,MMX,FXSR,SSE>
real memory  = 2147467264 (2097136K bytes)
sio0: gdb debugging port
avail memory = 2084040704 (2035196K bytes)
Preloaded elf kernel "kernel" at 0xc06d9000.
DEVFS: ready for devices
Pentium Pro MTRR support enabled
md0: Malloc disk
```

```
DRAM Data Integrity Mode: ECC Mode with h/w scrubbing
npx0: <math processor> on motherboard
npx0: INT 16 interface
pcib0: <ServerWorks NB6635 3.0LE host to PCI bridge> on motherboard
pci0: <PCI bus> on pcib0
pcic-pci0: <TI PCI-1410 PCI-CardBus Bridge> irq 15 at device 1.0 on pci0
pcic-pci0: TI12XX PCI Config Reg: [pwr save][pci only]
fxp0: <Intel Embedded 10/100 Ethernet> port 0x1000-0x103f mem
0xfb800000-0xfb81ffff,0xfb820000-0xfb820fff irq 9 at device 3.0 on pci0
fxp1: <Intel Embedded 10/100 Ethernet> port 0x1040-0x107f mem
0xfb840000-0xfb85ffff,0xfb821000-0xfb821fff irq 11 at device 4.0 on pci0
...
```

show system boot-messages (TX Matrix Plus Router)

```
user@host> show system boot-messages
sfc0-re0:
--------------------------------------------------------------------------
Copyright (c) 1996-2009, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
JUNOS 9.6B3.3 #0: 2009-06-17 19:52:08 UTC

builder@lanath.juniper.net:/volume/build/junos/9.6/release/9.6B3.3/obj-i386/bsd/sys/compile/JUNIPER
MPTable:  Timecounter "i8254" frequency 1193182 Hz quality 0 CPU: Intel(R) Xeon(R)
 CPU           L5238  @ 2.66GHz (2660.01-MHz 686-class CPU)   Origin =
"GenuineIntel"  Id = 0x1067a  Stepping = 10   Features=0xbfebfbff
...
lcc1-re0:
--------------------------------------------------------------------------
Copyright (c) 1996-2009, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
JUNOS 9.6-20090617.0 #0: 2009-06-17 04:15:14 UTC

builder@lanath.juniper.net:/volume/build/junos/9.6/production/20090617.0/obj-i386/bsd/sys/compile/JUNIPER
Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Intel(R) Xeon(R) CPU                 @ 1.86GHz (1862.01-MHz 686-class CPU)

  Origin = "GenuineIntel"  Id = 0x1067a  Stepping = 10
  Features=0xbfebfbff
...
```

show system boot-messages (QFX3500 Switch)

```
user@switch> show sytem boot-messages
getmemsize: msgbufp[size=32768] = 0x81d07fe4

System physical memory distribution:
-------------------------------------------------------------------------------
Total physical memory: 4160749568 (3968 MB)
Physical memory used: 3472883712 (3312 MB)
Physical memory allocated to kernel: 2130706432 (2032 MB)
Physical memory allocated to user BTLB: 1342177280 (1280 MB)
-------------------------------------------------------------------------------

Copyright (c) 1996-2010, Juniper Networks, Inc.
```

```
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
JUNOS 11.1I #0: 2010-09-17 19:18:07 UTC

ssiano@svl-junos-pool125.juniper.net:/c/ssiano/DEV_QFX_SI_BRANCH/03/20100917.399988/
obj-xlr/bsd/sys/compile/JUNIPER-DCTOR
WARNING: debug.mpsafenet forced to 0 as ipsec requires Giant
JUNOS 11.1I #0: 2010-09-17 19:18:07 UTC

ssiano@svl-junos-pool125.juniper.net:/c/ssiano/DEV_QFX_SI_BRANCH/03/20100917.399988/
obj-xlr/bsd/sys/compile/JUNIPER-DCTOR
real memory  = 3472883712 (3312MB)
avail memory = 1708171264 (1629MB)
cpuid: 0, btlb_cpumap:0xffffff8
FreeBSD/SMP: Multiprocessor System Detected: 12 CPUs
ETHERNET SOCKET BRIDGE initialising
Initializing QFX platform properties ..
cpu0 on motherboard
: RMI's XLR CPU Rev. 0.3 with no FPU implemented
        L1 Cache: I size 32kb(32 line), D size 32kb(32 line), eight way.
        L2 Cache: Size 1024kb, eight way
pic_lbus0: <XLR Local Bus>
pic_lbus0: <XLR Local Bus> on motherboard
Enter qfx control ethernet probe addr:0xc5eeec00
gmac4: <XLR GMAC GE Ethernet> on pic_lbus0
me0: Ethernet address 00:1d:b5:f7:68:40
Enter qfx control ethernet probe addr:0xc5eeeb40
gmac5: <XLR GMAC GE Ethernet> on pic_lbus0
me1: Ethernet address 00:1d:b5:f7:68:41
Enter qfx control ethernet probe addr:0xc5eeea80
gmac6: <XLR GMAC GE Ethernet> on pic_lbus0
me1: Ethernet address 00:1d:b5:f7:68:42
sio0 on pic_lbus0
Entering sioattach
sio0: type 16550A, console
xls_setup_intr: skip irq 3, xlr regs are set up somewhere else.
gblmem0 on pic_lbus0
ehci0: <RMI XLS USB 2.0 controller> on pic_lbus0
ehci_bus_attach: allocated resource.  tag=1, base=bef24000
xls_ehci_init: endian hardware swapping NOT enabled.
usb0: EHCI version 1.0
usb0 on ehci0
usb0: USB revision 2.0
uhub0: vendor 0x0000 EHCI root hub, class 9/0, rev 2.00/1.00, addr 1
uhub0: 2 ports with 2 removable, self powered
umass0: USB USBFlashDrive, rev 2.00/11.00, addr 2
pcib0: PCIe link 0 up
pcib0: PCIe link 2 up
pcib0: PCIe link 3 up
pcib0: <XLS PCI Host Controller> on pic_lbus0
pci0: <PCI bus> on pcib0
pcib1: <PCI-PCI bridge> at device 0.0 on pci0
pci1: <PCI bus> on pcib1
pci1: <network, ethernet> at device 0.0 (no driver attached)
pcib2: <PCI-PCI bridge> at device 1.0 on pci0
pcib3: <PCI-PCI bridge> at device 2.0 on pci0
pci2: <PCI bus> on pcib3
pci2: <network, ethernet> at device 0.0 (no driver attached)
pcib4: <PCI-PCI bridge> at device 3.0 on pci0
```



```
pci3: <PCI bus> on pcib4
pci3: <network, ethernet> at device 0.0 (no driver attached)
cfi device address space at 0xbc000000
cfi0: <AMD/Fujitsu - 8MB> on pic_lbus0
cfi device address space at 0xbc000000
i2c0: <I2C bus controller> on pic_lbus0
i2c1: <I2C bus controller> on pic_lbus0
qfx_fmn0 on pic_lbus0
pool offset 1503776768
xlr_lbus0: <XLR Local Bus Controller> on motherboard
qfx_bcpld_probe[124]
qfx_bcpld_probe[138]: dev_type=0x0
qfx_bcpld_probe[124]
qfx_bcpld0: QFX BCPLD probe success
qfx_bcpld0qfx_bcpld_attach[174]
qfx_bcpld_attach[207] : bus_space_tag=0x0, bus_space_handle=0xbd900000
qfx_bcpld_probe[124]
qfx_bcpld1: QFX BCPLD probe success
qfx_bcpld1qfx_bcpld_attach[174]
tor_bcpld_slave_attach[1245] : bus_space_tag=0x0, bus_space_handle=0xbda00000
Initializing product: 96 ..
bmeb: bmeb_lib_init done 0xc60a5000, addr 0x809c99a0
bme0:Virtual BME driver initializing
Timecounter "mips" frequency 1200000000 Hz quality 0
Timecounter "xlr_pic_timer" frequency 66666666 Hz quality 1
Timecounters tick every 1.000 msec
Loading the NETPFE fc module
IPsec: Initialized Security Association Processing.
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #7 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #11 Launched!
SMP: AP CPU #10 Launched!
SMP: AP CPU #9 Launched!
SMP: AP CPU #8 Launched!
da0 at umass-sim0 bus 0 target 0 lun 0
da0: <USB USBFlashDrive 1100> Removable Direct Access SCSI-0 device
da0: 40.000MB/s transfers
da0: 3920MB (8028160 512 byte sectors: 255H 63S/T 499C)
Trying to mount root from ufs:/dev/da0s1a
```

show system auto-snapshot

Syntax **show system auto-snapshot**

Release Information Command introduced in Junos OS Release 12.3 for EX Series switches.
Command introduced in Junos OS Release 12.1X45-D10 for SRX Series devices.

Description Display automatic snapshot status information. When the automatic snapshot feature is enabled and the system reboots from the alternate root partition, the switch automatically takes a snapshot of the root file system in the alternate root partition and copies it onto the primary root partition. This automatic snapshot procedure takes place whenever the system reboots from the alternate partition, regardless of whether the reboot from the alternate partition is due to a command or due to a corruption of the primary partition.

When the automatic snapshot procedure is in progress, you cannot run the manual snapshot command, **request system snapshot**.

Options This command has no options.

Required Privilege Level view

Related Documentation
- Understanding Resilient Dual-Root Partitions on Switches on page 93

List of Sample Output **show system auto-snapshot on page 427**

Output Fields Table 38 on page 413 describes the output fields for the **show system auto-snapshot** command. Output fields are listed in the approximate order in which they appear.

Table 41: show system auto-snapshot status Output Fields

Field Name	Field Description
Auto-snapshot configuration	Status of the configuration: • Enabled—If the system reboots from the alternate partition, the automatic snapshot feature automatically takes a snapshot of the alternate partition and copies it onto the primary partition. • Disabled—The system does not automatically take a snapshot of the alternate partition. You must use the manual snapshot command, **request system snapshot**, to take a snapshot of one partition and copy it onto the other.
Auto-snapshot state	Status of the automatic snapshot procedure: • **Completed**—The automatic snapshot procedure has completed copying the alternate partition to the primary partition and the alarm has been cleared. • **Disabled**—The automatic snapshot procedure is inactive. • **In progress**—The automatic snapshot procedure is in progress. It takes about 10 to 15 minutes to complete, depending upon disk size.

Sample Output

show system auto-snapshot

```
user@switch> show system auto-snapshot
Auto-snapshot Configuration: Enabled
Auto-snapshot State: Disabled
```

show system download

Syntax show system download *<download-id>*

Release Information Command introduced in Release 11.2 of Junos OS.

Description Display a brief summary of all the download instances along with their current state and extent of progress. If a **download-id** is provided, the command displays a detailed report of the particular download instance.

Options
- **download-id**—(Optional) The ID number of the download instance.

Required Privilege Level view

Related Documentation
- request system download start on page 348
- *Installation and Upgrade Guide*

List of Sample Output
show system download on page 428
show system download 1 on page 429

Output Fields Table 42 on page 428 lists the output fields for the **show system download** command. Output fields are listed in the approximate order in which they appear.

Table 42: show system download Output Fields

Field Name	Field Description
ID	Displays the download identification number.
Status	Displays the state of a particular download.
Start Time	Displays the start time of a particular download.
Progress	Displays the percentage of a download that has been completed.
URL	Displays the location of the downloaded file.

Sample Output

show system download

```
user@host> show system download
Download Status Information:
ID  Status      Start Time       Progress  URL
1   Active      May 4 06:28:36   5%        ftp://ftp-server//tftpboot/1m_file
2   Active      May 4 06:29:07   3%        ftp://ftp-server//tftpboot/5m_file
3   Error       May 4 06:29:22   Unknown   ftp://ftp-server//tftpboot/badfile
4   Completed   May 4 06:29:40   100%      ftp://ftp-server//tftpboot/smallfile
```


show system download 1

```
user@host> show system download 1

Download ID     : 1
Status          : Active
Progress        : 6%
URL             : ftp://ftp-server//tftpboot/1m_file
Local Path      : /var/tmp/1m_file
Maximum Rate    : 1k
Creation Time   : May 4 06:28:36
Scheduled Time  : May 4 06:28:36
Start Time      : May 4 06:28:37
Error Count     : 0
```

show system license

Syntax

show system license
<installed | keys | usage>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 13.3 for the MX104 3D Universal Edge Routers.

Description

Display licenses and information about how they are used.

Options

none—Display all license information.

installed—(Optional) Display installed licenses only.

keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.

usage—(Optional) Display the state of licensed features.

Required Privilege Level

maintenance

List of Sample Output

show system license on page 431
show system license installed on page 432
show system license keys on page 432
show system license usage on page 432
show system license (MX104 Routers) on page 432
show system license installed (MX104 Routers) on page 433
show system license keys (MX104 Routers) on page 433
show system license usage (MX104 Routers) on page 433
show system license (MX104 Routers) on page 433
show system license installed (MX104 Routers) on page 434
show system license keys (MX104 Routers) on page 434
show system license usage (MX104 Routers) on page 434
show system license (MX104 Routers) on page 435
show system license installed (MX104 Routers) on page 435
show system license keys (MX104 Routers) on page 435
show system license usage (MX104 Routers) on page 436
show system license (QFX Series) on page 436

Output Fields

Table 43 on page 430 lists the output fields for the **show system license** command. Output fields are listed in the approximate order in which they appear.

Table 43: show system license Output Fields

Field Name	Field Description
Feature name	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.

Table 43: show system license Output Fields *(continued)*

Field Name	Field Description
Licenses used	Number of licenses used by a router or switch. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used. NOTE: In Junos OS Release 10.1 and later, the **Licenses used** column displays the actual usage count based on the number of active sessions or connections as reported by the corresponding feature daemons. This is applicable for scalable license-based features such as Subscriber Access (**scale-subscriber**), L2TP (**scale-l2tp**), Mobile IP (**scale-mobile-ip**), and so on.
Licenses installed	Information about the installed license key: • **License identifier**—Identifier associated with a license key. • **State**—State of the license key:**valid** or **invalid**. An **invalid** state indicates that the key was entered incorrectly or is not valid for the specific device. • **License version**—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • **Valid for device**—Device that can use a license key. • **Group defined**—Group membership of a device. • **Features**—Feature associated with a license, such as data link switching (DLSw).
Licenses needed	Number of licenses required for features being used but not yet properly licensed.
Expiry	Amount of time left within the grace period before a license is required for a feature being used.

Sample Output

show system license

```
user@host> show system license

License usage:
                                  Licenses     Licenses    Licenses    Expiry
  Feature name                        used    installed      needed
  subscriber-accounting                  2            2           0    permanent
  subscriber-authentication              1            2           0    permanent
  subscriber-address-assignment          2            2           0    permanent
  subscriber-vlan                        2            2           0    permanent
  subscriber-ip                          0            2           0    permanent
  scale-subscriber                       2            3           0    permanent
  scale-l2tp                             4            5           0    permanent
  scale-mobile-ip                        1            2           0    permanent

Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    subscriber-accounting - Per Subscriber Radius Accounting
      permanent
    subscriber-authentication - Per Subscriber Radius Authentication
      permanent
    subscriber-address-assignment - Radius/SRC Address Pool Assignment
      permanent
    subscriber-vlan  - Dynamic Auto-sensed Vlan
```

```
      permanent
    subscriber-ip    - Dynamic and Static IP
      permanent
```

show system license installed

```
user@host> show system license installed
  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    subscriber-accounting - Per Subscriber Radius Accounting
      permanent
    subscriber-authentication - Per Subscriber Radius Authentication
      permanent
    subscriber-address-assignment - Radius/SRC Address Pool Assignment
      permanent
    subscriber-vlan  - Dynamic Auto-sensed Vlan
      permanent
    subscriber-ip    - Dynamic and Static IP
      permanent
```

show system license keys

```
user@host> show system license keys
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxx
```

show system license usage

```
user@host> show system license usage
License usage:
                                 Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  subscriber-accounting                 2            2           0    permanent
  subscriber-authentication             1            2           0    permanent
  subscriber-address-assignment         2            2           0    permanent
  subscriber-vlan                       2            2           0    permanent
  subscriber-ip                         0            2           0    permanent
  scale-subscriber                      2            3           0    permanent
  scale-l2tp                            4            5           0    permanent
  scale-mobile-ip                       1            2           0    permanent
```

show system license (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```
user@host> show system license
License usage:
                                 Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  scale-subscriber                      0         1000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  scale-mobile-ip                       0         1000           0    permanent
  MX104-2x10Gig-port-0-1                0            1           0    permanent

Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
  Features:
```

```
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent
```

show system license installed (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```
user@host > show system license installed
License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent
```

show system license keys (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```
user@host > show system license keys

XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxx
```

show system license usage (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```
user@host > show system license usage
           Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  scale-subscriber                      0         1000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  scale-mobile-ip                       0         1000           0    permanent
  MX104-2x10Gig-port-0-1                0            1           0    permanent
```

show system license (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                      used    installed      needed
  scale-subscriber                     0         1000           0    permanent
  scale-l2tp                           0         1000           0    permanent
  scale-mobile-ip                      0         1000           0    permanent
  MX104-2x10Gig-port-0-1               0            1           0    permanent
  MX104-2x10Gig-port-2-3               0            1           0    permanent

Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
```

```
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent

  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
      permanent
```

show system license installed (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license installed
License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent

  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
      permanent
```

show system license keys (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license keys

XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxx

XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxx
```

show system license usage (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license usage
           Licenses     Licenses    Licenses    Expiry
  Feature name                        used    installed      needed
  scale-subscriber                       0         1000           0    permanent
  scale-l2tp                             0         1000           0    permanent
```

```
  scale-mobile-ip                       0         1000           0    permanent
  MX104-2x10Gig-port-0-1                0            1           0    permanent
  MX104-2x10Gig-port-2-3                0            1           0    permanent
```

show system license (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license
License usage:
                                 Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  scale-subscriber                      0         1000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  scale-mobile-ip                       0         1000           0    permanent
  MX104-2x10Gig-port-0-1                0            1           0    permanent
  MX104-2x10Gig-port-2-3                0            1           0    permanent

Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent
    MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
      permanent
```

show system license installed (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license installed
License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent
    MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
      permanent
```

show system license keys (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license keys

XXXXXXXXX  xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx x
```

show system license usage (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license usage
           Licenses     Licenses    Licenses    Expiry
  Feature name                        used    installed      needed
  scale-subscriber                       0         1000           0    permanent
  scale-l2tp                             0         1000           0    permanent
  scale-mobile-ip                        0         1000           0    permanent
  MX104-2x10Gig-port-0-1                 0            1           0    permanent
  MX104-2x10Gig-port-2-3                 0            1           0    permanent
```

show system license (QFX Series)

```
user@switch> show system license
License usage:
                    Licenses     Licenses    Licenses    Expiry
  Feature name         used    installed      needed
  qfx-edge-fab            1            1           1    permanent
Licenses installed:
  License identifier: JUNOS417988
  License version: 1
  Features:
    qfx-edge-fab  -        QFX3000 Series QF/Node feature license
      permanent
```

show system license (SRX Series Services Gateways)

Syntax

show system license
<installed | keys | status | usage>

Release Information

Command introduced in Release 9.5 of Junos OS. Logical system status option added in Release 11.2 of Junos OS.

Description

Display licenses and information about how licenses are used.

Options

none—Display all license information.

installed—(Optional) Display installed licenses only.

keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.

status—(Optional) Display license status for a specified logical system or for all logical systems.

usage—(Optional) Display the state of licensed features.

Required Privilege Level

view

Related Documentation

- *Installation and Upgrade Guide*

List of Sample Output

show system license on page 438
show system license installed on page 438
show system license keys on page 439
show system license usage on page 439
show system license status logical-system all on page 439

Output Fields

Table 44 on page 437 lists the output fields for the **show system license** command. Output fields are listed in the approximate order in which they appear.

Table 44: show system license Output Fields

Field Name	Field Description
Feature name	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
Licenses used	Number of licenses used by the device. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used.

Table 44: show system license Output Fields *(continued)*

Field Name	Field Description
Licenses installed	Information about the installed license key: • **License identifier**—Identifier associated with a license key. • **License version**—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • **Valid for device**—Device that can use a license key. • **Features**—Feature associated with a license, such as data link switching (DLSw).
Licenses needed	Number of licenses required for features being used but not yet properly licensed.
Expiry	Time remaining in the grace period before a license is required for a feature being used.
Logical system license status	Displays whether a license is enabled for a logical system.

Sample Output

show system license

```
user@host> show system license

License usage:
                                 Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  av_key_kaspersky_engine               1            1           0    2012-03-30
 01:00:00 IST
  wf_key_surfcontrol_cpa                0            1           0    2012-03-30
 01:00:00 IST
  dynamic-vpn                           0            1           0    permanent
  ax411-wlan-ap                         0            2           0    permanent

Licenses installed:
  License identifier: JUNOS301998
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    av_key_kaspersky_engine - Kaspersky AV
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

  License identifier: JUNOS302000
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    wf_key_surfcontrol_cpa - Web Filtering
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license installed

```
user@host> show system license installed

License identifier: JUNOS301998
  License version: 2
  Valid for device: AG4909AA0080
  Features:
```

```
    av_key_kaspersky_engine - Kaspersky AV
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

  License identifier: JUNOS302000
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    wf_key_surfcontrol_cpa - Web Filtering
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license keys

```
user@host> show system license keys

XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxx
```

show system license usage

```
user@host> show system license usage

                                   Licenses     Licenses    Licenses  Expiry
Feature name                           used     installed      needed
  av_key_kaspersky_engine               1            1           0    2012-03-30
 01:00:00 IST
  wf_key_surfcontrol_cpa                0            1           0    2012-03-30
 01:00:00 IST
  dynamic-vpn                           0            1           0    permanent
  ax411-wlan-ap                         0            2           0    permanent
```

show system license status logical-system all

```
user@host> show system license status logical-system all
Logical system license status:

logical system name                 license status
root-logical-system                 enabled
LSYS0                               enabled
LSYS1                               enabled
LSYS2                               enabled
```

show system login lockout

Syntax show system login lockout

Release Information Command introduced in Junos OS Release 11.2.

Description Display the usernames locked after unsuccessful login attempts.

Required Privilege Level view and system

Related Documentation
- *lockout-period*
- clear system login lockout on page 341

List of Sample Output show system login lockout on page 440

Output Fields Table 45 on page 440 lists the output fields for the **show system login lockout** command. Output fields are listed in the approximate order in which they appear.

Table 45: show system login lockout

Field Name	Field Description	Level of Output
User	Username	All levels
Lockout start	Date and time the username was locked	All levels
Lockout end	Date and time the username was unlocked	All levels

Sample Output

show system login lockout

```
user@host> show system login lockout

User                 Lockout start           Lockout end
root                 2011-05-11 09:11:15 UTC 2011-05-11 09:13:15 UTC
```


show system snapshot

List of Syntax

Syntax on page 441
Syntax (EX Series Switches) on page 441

Syntax

show system snapshot

Syntax (EX Series Switches)

show system snapshot
<all-members|local|member *member-id*>
<media (external | internal)>

Release Information

Command introduced in Junos OS Release 7.6.
Command introduced in Junos OS Release 10.0 for EX Series switches.

Description

Display information about the backup software:

- On the routers, display information about the backup software, which is located in the **/altroot**, and **/altconfig** file systems or on the alternate media.
- On the switches, display information about the backup of the root file system **(/)** and directories **/altroot**,**/config**, **/var**, and **/var/tmp**, which are located either on an external USB flash drive or in internal flash memory.

NOTE: To back up software, use the **request system snapshot** command.

Options

none—Display information about the backup software.

all-members | local | member *member-id*—(EX Series switch Virtual Chassis only) (Optional) Display the snapshot in a Virtual Chassis:

- **all-members**—Display the snapshot for all members of the Virtual Chassis.
- **local**—Display the snapshot on the member of the Virtual Chassis that you are currently logged into.
- **member *member-id***—Display the snapshot for the specified member of the Virtual Chassis.

media (external | internal)—(EX Series switch only) (Optional) Display the destination media location for the snapshot. The **external** option specifies the snapshot on an external mass storage device, such as a USB flash drive. The **internal** option specifies the snapshot on an internal memory source, such as internal flash memory. If no additional options are specified, the command displays the snapshot stored in both slices.

Required Privilege Level

view

Related Documentation

- request system snapshot on page 365

List of Sample Output

show system snapshot (Router) on page 442
show system snapshot media external (Switch) on page 442
show system snapshot media internal (Switch) on page 443

Output Fields

Table 46 on page 442 lists the output fields for the **show system snapshot** command. Output fields are listed in the approximate order in which they appear.

Table 46: show system snapshot Output Fields

Field Name	Field Description
Creation date	Date and time of the last snapshot.
JUNOS version on snapshot	Junos OS release number of individual software packages.

Sample Output

show system snapshot (Router)

```
user@host> show system snapshot
Information for snapshot on hard-disk
Creation date: Oct 5 13:53:29 2005
JUNOS version on snapshot:
  jbase  : 7.3R2.5
  jcrypto: 7.3R2.5
  jdocs  : 7.3R2.5
  jkernel: 7.3R2.5
  jpfe   : M40-7.3R2.5
  jroute : 7.3R2.5
```

show system snapshot media external (Switch)

```
user@switch> show system snapshot media external
Information for snapshot on       external (/dev/da1s1a) (backup)
Creation date: Mar 19 03:37:18 2012
JUNOS version on snapshot:
  jbase  : ex-12.1I20120111_0048_user
  jcrypto-ex: 12.1I20120111_0048_user
  jdocs-ex: 12.1I20120111_0048_user
  jroute-ex: 12.1I20120111_0048_user
  jswitch-ex: 12.1I20120111_0048_user
  jweb-ex: 12.1I20120111_0048_user
Information for snapshot on       external (/dev/da1s2a) (primary)
Creation date: Mar 19 03:38:25 2012
JUNOS version on snapshot:
  jbase  : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
```

show system snapshot media internal (Switch)

```
user@switch> show system snapshot media internal
Information for snapshot on internal (/dev/da0s1a) (backup)
Creation date: Mar 14 05:01:02 2011
JUNOS version on snapshot:
  jbase  : 11.1R1.9
  jcrypto-ex: 11.1R1.9
  jdocs-ex: 11.1R1.9
  jkernel-ex: 11.1R1.9
  jroute-ex: 11.1R1.9
  jswitch-ex: 11.1R1.9
  jweb-ex: 11.1R1.9
  jpfe-ex42x: 11.1R1.9
Information for snapshot on internal (/dev/da0s2a) (primary)
Creation date: Mar 30 08:46:27 2011
JUNOS version on snapshot:
  jbase  : 11.2-20110330.0
  jcrypto-ex: 11.2-20110330.0
  jdocs-ex: 11.2-20110330.0
  jkernel-ex: 11.2-20110330.0
  jroute-ex: 11.2-20110330.0
  jswitch-ex: 11.2-20110330.0
  jweb-ex: 11.2-20110330.0
  jpfe-ex42x: 11.2-20110330.0
```

show system snapshot media

Syntax show system snapshot media *media-type*

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the snapshot information for both root partitions on SRX Series devices

Options

- internal— Show snapshot information from internal media.
- usb— Show snapshot information from device connected to USB port.
- external— Show snapshot information from the external compact flash. This option is available on the SRX650 Services Gateway.

Required Privilege Level View

Related Documentation

- *Installation and Upgrade Guide*

show system snapshot media internal

show system snapshot media internal

```
Information for snapshot on       internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
  junos  : 10.1B3-domestic
Information for snapshot on       internal (/dev/da0s2a) (backup)
Creation date: Jan 15 10:15:32 2010
JUNOS version on snapshot:
  junos  : 10.2-20100112.0-domestic
```

show system snapshot media usb

show system snapshot media usb

```
Information for snapshot on       usb (/dev/da1s1a) (primary)
            Creation date: Jul 24 16:16:01 2009
            JUNOS version on snapshot:
            junos  : 10.0I20090723_1017-domestic
            Information for snapshot on       usb (/dev/da1s2a) (backup)
            Creation date: Jul 24 16:17:13 2009
            JUNOS version on snapshot:
            junos  : 10.0I20090724_0719-domestic
```

request system software abort in-service-upgrade (ICU)

Syntax request system software abort in-service-upgrade

Release Information Command introduced in Release 11.2 of Junos OS.

Description Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the **request system in-service-upgrade** command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.

Options This command has no options.

Required Privilege Level view

Related Documentation

- *request system software in-service-upgrade (Maintenance)*

List of Sample Output request system software abort in-service-upgrade on page 445

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software abort in-service-upgrade

```
user@host> request system software abort in-service-upgrade
In-Service-Upgrade aborted
```

show system storage partitions (EX Series Switches Only)

Syntax

show system storage partitions
<all-members>
<local>
<member *member-id*>

Release Information

Command introduced in Junos OS Release 11.1 for EX Series switches.

Description

Display information about the disk partitions on EX Series switches.

Options

none—Display partition information.

all-members—(Virtual Chassis systems only) (Optional) Display partition information for all members of the Virtual Chassis.

local—(Virtual Chassis systems only) (Optional) Display partition information for the local Virtual Chassis member.

member *member-id*—(Virtual Chassis systems only) (Optional) Display partition information for the specified member of the Virtual Chassis configuration.

Required Privilege Level

view

Related Documentation

- Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 180

List of Sample Output

show system storage partitions on page 447

Output Fields

Table 47 on page 446 describes the output fields for the **show system storage partitions** command. Output fields are listed in the approximate order in which they appear.

Table 47: show system storage partitions Output Fields

Field Name	Field Description
Boot Media	Media (internal or external) from which the switch was booted.
Active Partition	Name of the active root partition.
Backup Partition	Name of the backup (alternate) root partition.
Currently booted from	Partition from which the switch was last booted.
Partitions information	Information about partitions on the boot media: • Partition—Partition identifier. • Size—Size of partition. • Mountpoint—Directory on which the partition is mounted.

Sample Output

show system storage partitions

```
user@switch> show system storage partitions
fpc0:
--------------------------------------------------------------------------
Boot Media: internal (da0)
Active Partition: da0s1a
Backup Partition: da0s2a
Currently booted from: active (da0s1a)

Partitions information:
  Partition  Size   Mountpoint
  s1a        184M   /
  s2a        184M   altroot
  s3d        369M   /var/tmp
  s3e        123M   /var
  s4d        62M    /config
  s4e               unused (backup config)
```

show system storage partitions (View SRX Series)

Syntax show system storage partitions

Release Information Command introduced in Release 10.2 of Junos OS.

Description Displays the partitioning scheme details on SRX Series devices.

Required Privilege Level View

Related Documentation
- *Installation and Upgrade Guide*

show system storage partitions (dual root partitioning)

show system storage partitions

```
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   altroot
      s2a    293M   /
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```

show system storage partitions (single root partitioning)

show system storage partitions

```
Boot Media: internal (da0)
Partitions Information:
  Partition  Size   Mountpoint
      s1a    898M   /
      s1e    24M    /config
      s1f    61M    /var
```

show system storage partitions (USB)

show system storage partitions

```
Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   /
      s2a    293M   altroot
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```

PART 6

Index

Index

Symbols

A

B

C

D

E

F

H

I

J

L

M

S

T

U

V