



Junos[®] OS

Installation and Upgrade Guide

Release
15.1



Modified: 2016-11-13

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] OS Installation and Upgrade Guide

15.1

Copyright © 2016, Juniper Networks, Inc.

All rights reserved.

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

	About the Documentation	xix
	Documentation and Release Notes	xix
	Supported Platforms	xix
	Using the Examples in This Manual	xx
	Merging a Full Example	xx
	Merging a Snippet	xxi
	Documentation Conventions	xxi
	Documentation Feedback	xxiii
	Requesting Technical Support	xxiv
	Self-Help Online Tools and Resources	xxiv
	Opening a Case with JTAC	xxiv
Part 1	Junos Software and Hardware Overview	
Chapter 1	Software Overview	3
	Junos OS Overview	3
	One Operating System	4
	One Modular Software Architecture	4
	Junos OS Editions	5
	FIPS 140-2 Security Compliance	5
	Junos OS Installation Packages	6
	Junos OS Package Names for EX Series Switches	7
	Software Naming Convention	9
	Software Naming Convention for SRX Series Devices	10
	Software Package Information Security	11
	Junos OS Release Numbers	11
	Installation Media	12
	Installation Bundles	13
	Installation Modules	14
	Configuration Files	15
	Configuration File Selection Sequence	15
	Remote Storage of Configuration Files	16
	Understanding Software Infrastructure and Processes	17
	Routing Engine and Packet Forwarding Engine	17
	Junos OS Processes	17
	Understanding Junos OS with Upgraded FreeBSD	19
	Understanding Junos OS with Upgraded FreeBSD Package Names	22
	Understanding Junos OS with Upgraded FreeBSD Snapshots	23
	Understanding Junos OS with Upgraded FreeBSD Disk Volumes	24

Chapter 2	Hardware Overview	27
	Hardware Architecture Overview	27
	Hardware Overview (ACX Series, M Series, MX Series, T Series, and TX Matrix Routers)	28
	System Memory	29
	Storage Media	30
	Hardware Overview of SRX Series Services Gateways	31
	SRX Series Device Overview	31
	System Memory	31
	Storage Media	32
	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)	32
	Storage Media Names for SRX Series Devices	34
	Boot Sequence on M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series Devices with Routing Engines	35
	Boot Sequence on SRX Series Devices	37
Part 2	Installing Junos Software	
Chapter 3	Installation Overview	41
	Installation Type Overview	41
	Standard Installation	41
	Category Change Installation	41
	Recovery Installation	42
	Installation Categories on the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus Routers	42
	Installation Categories on SRX Series Devices	43
	Understanding Software Installation on EX Series Switches	44
	Overview of the Software Installation Process	44
	Software Package Security	44
	Installing Software on a Virtual Chassis	45
	Installing Software on Switches with Redundant Routing Engines	45
	Installing Software Using Automatic Software Download	45
	Autoinstalling a Configuration File on an EX2200 or EX3300 Switch from a Disk-on-Key USB Memory Stick	46
	Installing Software on an EX2300 or EX3400 Switch	46
	Troubleshooting Software Installation	46
Chapter 4	Performing a Standard or Change Category Installation	47
	Checking the Current Configuration and Candidate Software Compatibility	47
	Determining the Junos OS Version	48
	Downloading Software	48
	Downloading Software with a Browser	49
	Downloading Software Using the Command-Line Interface	49
	Downloading Software Packages from Juniper Networks	51
	Understanding Download Manager for SRX Series Devices	51
	Overview	51
	Using Download Manager to Upgrade Junos OS	52
	Handling Errors	52

	Considerations	53
	Understanding the Console Port	53
	Backing Up the Existing Installation on Routers	55
	Backing Up the Current Installation on SRX Series Devices	56
	Backing Up the Current Installation on High-End SRX Series Devices	56
	Backing Up the Current Installation on Branch SRX Series Devices	57
	Installing the Software Package on a Router with a Single Routing Engine	57
	Installing the Software Package on a Router with Redundant Routing Engines	58
	Preparing the Router for the Installation	59
	Installing Software on the Backup Routing Engine	59
	Installing Software on the Master Routing Engine	61
	Finalizing the Installation	63
	Repartitioning Routing Engine System Storage To Increase the Swap Partition	64
	Installing Software on EX Series Switches (J-Web Procedure)	64
	Installing Software Upgrades from a Server	65
	Installing Software Upgrades by Uploading Files	65
	Registering the EX Series Switch with the J-Web Interface	66
	Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices	66
	Installing Junos OS on SRX Series Devices Using a USB Flash Drive	68
	Upgrading the Boot Loader on SRX Series Devices	69
	Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server	70
	Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device	72
Chapter 5	Configuring Zero Touch Provisioning	73
	Understanding Zero Touch Provisioning	73
	Configuring Zero Touch Provisioning	76
Chapter 6	Configuring Automatic Installation of Configuration Files	81
	Autoinstallation Overview	81
	Automatic Installation of Configuration Files	82
	Supported Autoinstallation Interfaces and Protocols	82
	Typical Autoinstallation Process on a New Device	83
	Example: Configuring Autoinstallation on SRX Series Devices	84
	Configuring Autoinstallation on JNU Satellite Devices	87
	Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group	89
	Supported Autoinstallation Interfaces and Protocols	89
	Typical Autoinstallation Process on a New Router	90
	Autoinstallation of Satellite Devices in a Junos Node Unifier Group	91
	Verifying Autoinstallation on JNU Satellite Devices	92
Chapter 7	Configuring Dual-Root Partitions for High Availability	95
	Understanding Resilient Dual-Root Partitions on Switches	95
	Resilient Dual-Root Partition Scheme (Junos OS Release 10.4R3 and Later)	96
	Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature	96

Earlier Partition Scheme (Junos OS Release 10.4R2 and Earlier)	97
Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases	98
Resilient Dual-Root Partitions Frequently Asked Questions	99
How Does Upgrading to Junos OS Release 10.4R3 and Later Differ from Normal Upgrades?	99
What Happens If I Do Not Upgrade Both the Loader Software and Junos OS at the Same Time?	100
Can I Downgrade Junos OS Without Downgrading the Loader Software?	101
Can I Upgrade to a Resilient Dual-Root Partition Release by Using the CLI?	101
Will I Lose My Configuration During an Upgrade?	102
How Long Will the Upgrade Process Take?	102
What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Enabled?	102
What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Not Enabled?	103
How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System?	103
Can I Use Automatic Software Update and Download to Upgrade to a Resilient Dual-Root Partition Release?	104
Why Is the Message "At least one package installed on this device has limited support" Displayed When Users Log In to a Switch?	104
Where Can I Find Instructions for Upgrading?	104
Dual-Root Partitioning Scheme on SRX Series Devices	105
Boot Media and Boot Partition on SRX Series Devices	106
Important Features of the Dual-Root Partitioning Scheme	106
Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning	106
Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers Devices	108
Understanding How Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning	109
Example: Installing Junos OS on SRX Series Devices Using the Partition Option	110
Chapter 8 Upgrading Software	115
Upgrading Software Packages	116
Upgrading to 64-bit Junos OS	119
Upgrading Routers Using Unified ISSU	122
Understanding Nonstop Software Upgrade on EX Series Switches	123
Requirements for Performing an NSSU	124
How an NSSU Works	125
EX3300, EX4200, EX4300, EX4500, and Mixed Virtual Chassis	125
EX6200 and EX8200 Switches	126
EX8200 Virtual Chassis	127
NSSU Limitations	128
NSSU and Junos OS Release Support	128

Overview of NSSU Configuration and Operation	129
Upgrading Software by Using Automatic Software Download	129
Verifying That Automatic Software Download Is Working Correctly	131
Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch	131
Verifying the Number of Partitions and File System Mountings	132
Verifying the Loader Software Version	132
Verifying Which Root Partition Is Active	133
Verifying the Junos OS Version in Each Root Partition	134
Upgrading the Loader Software on the Line Cards in a Standalone EX8200 Switch or an EX8200 Virtual Chassis	136
Upgrading Junos OS with Upgraded FreeBSD	139
To Install Junos OS with Upgraded FreeBSD Over a Plain Junos OS	141
To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of an Earlier Release	144
To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of a Later Release	145
Understanding Junos OS Upgrades for SRX Series Devices	145
Understanding Junos OS Upgrades	146
Junos OS Upgrade Methods on the SRX Series Devices	146
Preparing Your SRX Series Device for Junos OS Upgrades	147
Secondary Storage Devices Available on SRX Series Devices	147
Verifying Available Disk Space on SRX Series Devices	148
Cleaning Up the System File Storage Space	149
Downloading Software Packages from Juniper Networks	150
Example: Installing Junos OS Upgrade Packages on SRX Series Devices	150
Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server	153
Understanding BIOS Upgrades on SRX Series Devices	154
Understanding Manual BIOS Upgrade Using the Junos CLI	154
Understanding Auto BIOS Upgrade Methods on SRX Series Devices	155
Disabling Auto BIOS Upgrade on SRX Series Devices	156
Example: Downgrading Junos OS on SRX Series Devices	156
Chapter 9	
Booting a Device Using a System Snapshot	159
Understanding System Snapshot on EX Series Switches	159
Creating a Snapshot and Using It to Boot an EX Series Switch	160
Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch	160
Verifying That a System Snapshot Was Created on an EX Series Switch	161
Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive	162

Chapter 10	Performing a Recovery Installation	165
	Creating an Emergency Boot Device	165
	Configuring Boot Devices for SRX Series Devices	166
	Example: Creating a Snapshot and Using It to Boot an SRX Series Device	166
	Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices	169
	Overview	170
	How Autorecovery Works	170
	How to Use Autorecovery	170
	Data That Is Backed Up in an Autorecovery	171
	Troubleshooting Alarms	171
	Considerations	171
	Performing a Recovery Installation	172
	Creating a New Configuration on a Single Routing Engine	173
	Log In to the Router Console	173
	Configure Administration User Accounts	174
	Add the Management Console to the Network	174
	Commit Changes	176
	Creating a New Configuration with Redundant Routing Engines	178
	Configure Administration User Accounts	178
	Set Up Routing Engine Configuration Groups	179
	Complete the Management Console Configuration	180
	Commit and Synchronize Changes	181
	Saving a Rescue Configuration File	183
	Restoring a Saved Configuration	184
	Copy Saved Files to the Router	184
	Loading and Committing the Configuration File	185
	Reverting to the Default Factory Configuration by Using the request system zeroize Command	185
	Reverting to the Rescue Configuration	186
Chapter 11	Reinstalling Software	187
	Checklist for Reinstalling Junos OS	187
	Log the Software Version Information	189
	Log the Hardware Version Information	190
	Log the Chassis Environment Information	191
	Log the System Boot-Message Information	192
	Log the Active Configuration	194
	Log the Interfaces on the Router	194
	Log the BGP, IS-IS, and OSPF Adjacency Information	195
	Log the System Storage Information	196
	Back Up the Currently Running and Active File System	197

	Reinstall Junos OS	197
	Reconfigure Junos OS	198
	Configure Host Names, Domain Names, and IP Addresses	198
	Protecting Network Security by Configuring the Root Password	200
	Check Network Connectivity	201
	Copy Backup Configurations to the Router	202
	Configure Host Names, Domain Names, and IP Addresses	202
	Protecting Network Security by Configuring the Root Password	204
	Check Network Connectivity	206
	Copy Backup Configurations to the Router	206
	After You Reinstall Junos OS	206
	Compare Information Logged Before and After the Reinstall	206
	Back Up the New Software	207
	Compare Information Logged Before and After the Reinstall	207
	Back Up the New Software	207
Chapter 12	Downgrading Software	209
	Downgrading Junos OS from Upgraded FreeBSD	209
	Downgrading from Junos OS with Upgraded FreeBSD to Junos OS	209
	Downgrading from Junos OS with Upgraded FreeBSD to an Earlier Release of Junos OS with Upgraded FreeBSD	211
Chapter 13	Rebooting or Halting Software Processes on a Device	213
	Restarting and Halting SRX Series Devices	213
	Rebooting SRX Series Devices	213
	Halting SRX Series Devices	215
	Bringing Chassis Components Online and Offline on SRX Series Devices	217
	Restarting the Chassis on SRX Series Devices	217
	Rebooting or Halting the EX Series Switch (J-Web Procedure)	218
Part 3	Installing and Managing Software Licenses	
Chapter 14	Software License Overview	221
	Junos OS Feature Licenses	221
	License Enforcement	222
	Junos OS Feature License Keys	223
	Release-Tied License Keys and Upgrade Licenses on MX Series Routers	223
	Licensable Ports on MX5, MX10, and MX40 Routers	224
	Port Activation on MX104 Routers	225
	Software Feature Licenses	226
	Software Features That Require Licenses on M Series, MX Series, and T Series Routers	226
	Software Features That Require Licenses on M Series Routers Only	229
	Software Features That Require Licenses on MX Series Routers Only	230
	Software Feature Licenses for SRX Series Devices	234
	Software Features That Require Licenses on EX Series Switches	239
	Software Features That Require Licenses on the QFX Series	241
	Understanding Software Licenses for EX Series Switches	244
	Purchasing a Software Feature License	244
	Features Requiring a License on EX2200 Switches	245

	Features Requiring a License on EX2300 Switches	246
	Features Requiring a License on EX3300 Switches	246
	Features Requiring a License on EX3400 Switches	247
	Features Requiring a License on EX4300 Switches	248
	Features Requiring a License on EX4600 Switches	250
	Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches	251
	License Warning Messages	252
Chapter 15	Installing and Managing Licenses	255
	Adding New Licenses (CLI Procedure)	255
	Deleting a License (CLI Procedure)	256
	Saving License Keys	257
	Verifying Junos OS License Installation	258
	Displaying Installed Licenses	258
	Displaying License Usage	259
Part 4	Troubleshooting Information	
Chapter 16	Troubleshooting Software Installation	263
	Troubleshooting Software Installation	263
	Recovering from a Failed Software Upgrade on an EX Series Switch	263
	Rebooting from the Inactive Partition	264
	Freeing Disk Space for Software Installation	265
	Installation from the Boot Loader Generates 'cannot open package' Error	265
	Troubleshooting a Switch That Has Booted from the Backup Junos OS Image	266
	Disk Space Management for Junos OS Installation	267
	Verifying PIC Combinations	267
Part 5	Configuration Statements and Operational Commands	
Chapter 17	Configuration Statements	271
	auto-configuration	272
	auto-configuration (System)	273
	auto-image-upgrade	275
	auto-snapshot	276
	autoinstallation	277
	autoinstallation (JNU Satellite Devices)	278
	bootp	279
	commit	280
	configuration-servers	281
	delete-after-commit (JNU Satellites)	282
	interfaces (Autoinstallation)	283
	license	284
	usb	286
	usb-control	286

Chapter 18	Operational Commands	287
	clear system login lockout	289
	request system autorecovery state	290
	request system download abort	292
	request system download clear	293
	request system download pause	294
	request system download resume	295
	request system download start	296
	request system firmware upgrade	297
	request system halt	298
	request system license add	300
	request system license delete	301
	request system license save	302
	request system license update	303
	request system partition compact-flash	304
	request system power-off	305
	request system reboot	307
	request system reboot	312
	request system reboot (Junos OS with Upgraded FreeBSD)	314
	request system scripts add	317
	request system scripts delete	318
	request system scripts rollback	319
	request system snapshot	320
	request system snapshot (Junos OS with Upgraded FreeBSD)	327
	request system snapshot (SRX Series)	329
	request system software abort in-service-upgrade (ICU)	331
	request system software add	332
	request system software add (Maintenance)	342
	request system software configuration-backup	343
	request system software configuration-restore	344
	request system software delete	345
	request system software rollback	349
	request system software rollback (SRX Series)	354
	request system software validate	355
	request system software validate on (Junos OS with Upgraded FreeBSD)	359
	request system storage cleanup	362
	request system storage cleanup (SRX Series)	372
	request system zeroize	375
	show chassis usb storage	380
	show system autoinstallation status	381
	show system autorecovery state	383
	show system boot-messages	385
	show system auto-snapshot	392
	show system download	394
	show system license	396
	show system license (View)	404
	show system login lockout	407
	show system snapshot	408
	show system snapshot (Junos OS with Upgraded FreeBSD)	411

show system snapshot media	412
show system storage partitions (EX Series Switches Only)	413
show system storage partitions (View SRX Series)	415

Part 6

Index

Index	419
-------------	-----

List of Figures

Part 1	Junos Software and Hardware Overview	
Chapter 1	Software Overview	3
	Figure 1: Configuration Selection Sequence	15
Chapter 2	Hardware Overview	27
	Figure 2: Routing Engines	29
	Figure 3: SRX345 Device Front Panel	31
	Figure 4: SRX1500 Device Front Panel	31
	Figure 5: SRX5800 Device Routing Engine	31
	Figure 6: SRX4200 Services Gateway Front Panel	31
Part 2	Installing Junos Software	
Chapter 4	Performing a Standard or Change Category Installation	47
	Figure 7: Connecting to the Console Port on a Junos OS Device	54
Chapter 8	Upgrading Software	115
	Figure 8: Upgrading to the 64-bit Junos OS with Dual Routing Engines	120
	Figure 9: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master in Either Slot)	121
	Figure 10: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master Must Be in Slot 0)	122

List of Tables

	About the Documentation	xix
	Table 1: Notice Icons	xxii
	Table 2: Text and Syntax Conventions	xxii
Part 1	Junos Software and Hardware Overview	
Chapter 1	Software Overview	3
	Table 3: Junos OS Processes	18
	Table 4: Upgraded FreeBSD Kernel Support by Hardware Platform	19
	Table 5: New and Changed Commands and Statements for Junos OS with Upgraded FreeBSD	20
	Table 6: Deprecated Commands and Statements for Junos OS with Upgraded FreeBSD	21
Chapter 2	Hardware Overview	27
	Table 7: Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers)	33
	Table 8: Storage Media Names	34
Part 2	Installing Junos Software	
Chapter 4	Performing a Standard or Change Category Installation	47
	Table 9: show system download Output Fields	53
	Table 10: Install Remote Summary	65
	Table 11: Upload Package Summary	66
	Table 12: Environment Variables Settings	71
Chapter 6	Configuring Automatic Installation of Configuration Files	81
	Table 13: Interfaces and Protocols for IP Address Acquisition During Autoinstallation	82
Chapter 7	Configuring Dual-Root Partitions for High Availability	95
	Table 14: Resilient Dual-Root Partition Scheme	96
	Table 15: Earlier Partition Scheme	98
	Table 16: Combinations of Junos OS Versions and Loader Software Versions	100
	Table 17: Actions If Corrupt Files Are Found and Automatic Snapshot is Enabled	102
	Table 18: Actions If Corrupt Files Are Found	103
	Table 19: Storage Media on SRX Series Devices	106
Chapter 8	Upgrading Software	115
	Table 20: Platform and Release Support for NSSU	128

	Table 21: Upgrade Path to Junos OS with the Upgraded FreeBSD	139
	Table 22: Secondary Storage Devices for SRX Series Devices	148
	Table 23: Install Package Summary	153
	Table 24: CLI Commands for Manual BIOS Upgrade	154
Chapter 10	Performing a Recovery Installation	165
	Table 25: Autorecovery Alarms	171
Chapter 11	Reinstalling Software	187
	Table 26: Checklist for Reinstalling Junos OS	187
Part 3	Installing and Managing Software Licenses	
Chapter 14	Software License Overview	221
	Table 27: Upgrade Licenses for Enhancing Port Capacity	225
	Table 28: Port Activation License Model for MX104 Routers	226
	Table 29: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers	227
	Table 30: Junos OS Feature License Model Number for M Series Routers	230
	Table 31: Junos OS Feature License Model Number for MX Series Routers	231
	Table 32: Junos OS Feature Licenses	234
	Table 33: Junos OS Feature License Model Number for SRX Series Devices	236
	Table 34: Junos OS Enhanced Feature License (EFL) and Advanced Feature License (AFL) Model Number for EX Series Devices	240
	Table 35: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices	242
	Table 36: Junos OS EFL Part Number on EX2200 Switches	245
	Table 37: Junos OS EFL Part Number on EX2300 Switches	246
	Table 38: Junos OS EFL Part Number on EX3300 Switches	247
	Table 39: Junos OS AFL Part Number on EX3300 Switches	247
	Table 40: Junos OS EFL Part Number on EX3400 Switches	248
	Table 41: Junos OS EFL Part Number on EX4300 Switches	249
	Table 42: Junos OS AFL Part Number on EX4300 Switches	249
	Table 43: Junos OS AFL Part Number on EX4600 Switches	250
	Table 44: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches	251
Part 5	Configuration Statements and Operational Commands	
Chapter 18	Operational Commands	287
	Table 45: request system storage cleanup Output Fields	364
	Table 46: request system storage cleanup Output Fields	372
	Table 47: show system autoinstallation status Output Fields	381
	Table 48: show system autorecovery state Output Fields	383
	Table 49: show system auto-snapshot status Output Fields	392
	Table 50: show system download Output Fields	394
	Table 51: show system license Output Fields	397
	Table 52: show system license Output Fields	404
	Table 53: show system login lockout	407
	Table 54: show system snapshot Output Fields	409

Table 55: show system storage partitions Output Fields 413

About the Documentation

- Documentation and Release Notes on page xix
- Supported Platforms on page xix
- Using the Examples in This Manual on page xx
- Documentation Conventions on page xxi
- Documentation Feedback on page xxiii
- Requesting Technical Support on page xxiv

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
- EX Series
- PTX Series
- QFabric System
- QFX Series
- 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.xml; }
```

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 [CLI Explorer](#).

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
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	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 <i>domain-name</i>

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.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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 [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; 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.	<ul style="list-style-type: none"> 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

- [Software Overview on page 3](#)
- [Hardware Overview on page 27](#)

CHAPTER 1

Software Overview

- [Junos OS Overview on page 3](#)
- [Junos OS Editions on page 5](#)
- [FIPS 140-2 Security Compliance on page 5](#)
- [Junos OS Installation Packages on page 6](#)
- [Junos OS Package Names for EX Series Switches on page 7](#)
- [Software Naming Convention on page 9](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)
- [Software Package Information Security on page 11](#)
- [Junos OS Release Numbers on page 11](#)
- [Installation Media on page 12](#)
- [Installation Bundles on page 13](#)
- [Installation Modules on page 14](#)
- [Configuration Files on page 15](#)
- [Understanding Software Infrastructure and Processes on page 17](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)
- [Understanding Junos OS with Upgraded FreeBSD Snapshots on page 23](#)
- [Understanding Junos OS with Upgraded FreeBSD Disk Volumes on page 24](#)

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.

Starting with Junos OS Release 15.1, certain hardware platforms run Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. Basing Junos OS on the newer kernel (referred to as Junos OS with upgraded FreeBSD) provides Junos OS with sophisticated processing, efficiency, and security features which do not have to be reproduced in Junos OS.

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 on page 4](#)
- [One Modular Software Architecture on page 4](#)

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 5](#)
- [Junos OS Installation Packages on page 6](#)

Junos OS Editions



NOTE: Hardware platforms running Junos OS with the upgraded FreeBSD kernel employ a new naming scheme for software packages that does not recognize different major software package categories, such as domestic, world-wide, or Federal Information Processing Standard (FIPS). For more information, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

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](#).

Related Documentation

- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)

FIPS 140-2 Security Compliance



NOTE: Hardware platforms running Junos OS with the upgraded FreeBSD kernel employ a new naming scheme for software packages that does not recognize different major software package categories, such as domestic, world-wide, or Federal Information Processing Standard (FIPS). For more information, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

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.

Related Documentation

- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)

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:



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. Junos OS with upgraded FreeBSD has a different, simplified package naming convention. For more information, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

Installation Package	Description
jinstall*	Junos OS for M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers.
jinstall-ppc*	Junos OS for the ACX Series, MX80, and MX104 routers.
jinstall-ex*	Junos OS for the EX Series Ethernet Switch portfolio.

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-srxentedge*	Junos OS for SRX1500
junos-srx5000*	Junos OS for SRX5400, SRX5600 and SRX5800.
junos-srxmr*	Junos OS for SRX4100 and SRX4200

Related Documentation

- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)

Junos OS Package Names for EX Series Switches

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 \(CLI Procedure\)](#)
- [Installing Software on an EX Series Switch with Redundant Routing Engines \(CLI Procedure\)](#)
- [Downloading Software Packages from Juniper Networks on page 51](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)

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.

All SRX Series packages conform to the following naming convention:

junos-product-release-edition

For example:

junos-srxentedge-15.1X49-D30.3-domestic.tgz (for SRX1500)

junos-vsrx-15.1X49-D30.3-domestic.tgz (for vSRX)

junos-srx5000-15.1X49-D30.3-domestic.tgz (for SRX5400, SRX5600, SRX5800)

junos-srxsme-15.1X49-D30.3-domestic.tgz (for SRX550M)

junos-srxsmr-15.1X49-D65.5-domestic.tgz (for SRX4100 and SRX4200)

where:

- **product** means SRX Series product line.
- **edition** means 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 device.



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). Junos OS with upgraded FreeBSD has a new naming convention. For more information on this new naming convention, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

Related Documentation

- [Software Naming Convention for SRX Series Devices on page 10](#)
- [Junos OS Release Numbers on page 11](#)
- [FIPS 140-2 Security Compliance on page 5](#)

- [Junos OS Editions on page 5](#)

Software Naming Convention for SRX 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.

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.

For more information, see [“Junos OS Release Numbers” on page 11](#).



NOTE: Starting with Junos OS Release 12.1X44-D10, SRX Series devices follow a special naming convention for Junos OS releases. For more information, refer to the Knowledge Base article KB30092 at <http://kb.juniper.net/InfoCenter/index?page=home>.

- **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-srxentedge-15.1X49-D30.3-domestic.tgz (For SRX1500 devices)
- junos-srxmr-15.1X49-D65.5-domestic.tgz (For SRX4100 and SRX4200 devices)

Related Documentation

- [FIPS 140-2 Security Compliance on page 5](#)
- [Junos OS Release Numbers on page 11](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)

Software Package Information Security

Junos OS software 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.

Related Documentation

- [Installation Type Overview on page 41](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)

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 14.1,14.2, or 15.1. 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 webpage, 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:

14.2R3.2

Where:

- *m* is the main 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
 - *F*— Feature Velocity release software



NOTE: Feature velocity release was introduced in Junos OS Release 15.1.

- *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: Releases that follow a numbering system that differs from the standard Junos OS release numbering.

Starting with Junos OS Release 12.1X44-D10, SRX Series devices follow a special naming convention for Junos OS releases. For more information, refer to the Knowledge Base article KB30092 at

<http://kb.juniper.net/InfoCenter/index?page=home>.

- *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

- For Service release software, the release number is added at the end. For example, 14.2R3-S4.4. Here S4 represents the 4th service release on top of 14.2R3 and is the 4th respin.



NOTE: Prior to Junos OS Release 11.4, the software release number format for service releases was same as other releases. For example, 10.4S4.2 represented the 4th service release and 2nd respin of 10.4.



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). Junos OS with upgraded FreeBSD has a new naming convention. For more information on this new naming convention, see “[Understanding Junos OS with Upgraded FreeBSD Package Names](#)” on page 22.

Related Documentation

- [Junos OS Installation Packages on page 6](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)
- [Junos OS Editions 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.



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 a USB Flash Drive” on page 68](#) and [“Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server” on page 70](#).

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.



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). Junos OS with upgraded FreeBSD has a new naming convention. For more information on this new naming convention, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

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
kernel*	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.
crypto*	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, and TX Matrix Plus routers.



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). Junos OS with upgraded FreeBSD has a new naming convention. For more information on this new naming convention, see [“Understanding Junos OS with Upgraded FreeBSD Package Names”](#) on page 22.

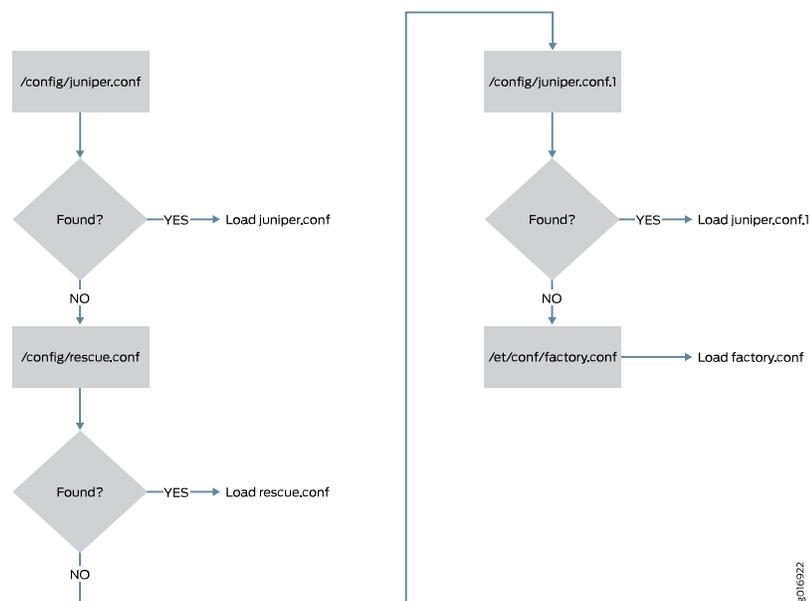
Configuration Files

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 15.

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 ["Loading and Committing the Configuration File" on page 185](#).

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

- Related Documentation**
- [Installation Modules on page 14](#)

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 17](#)
- [Junos OS Processes on page 17](#)

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 18](#) describes the primary Junos OS processes.

Table 3: Junos OS Processes

Process	Name	Description
Chassis process	chassisd	<p>Detects hardware on the system that is used to configure network interfaces.</p> <p>Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered.</p> <p>Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</p>
Ethernet switching process	eswd	<p>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.</p> <p>Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</p> <p>NOTE: The process is not applicable for EX2300 and EX3400 switches</p>
Forwarding process	pfem	<p>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</p>
Interface process	dcd	<p>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</p>
Management process	mgd	<p>Provides communication between the other processes and an interface to the configuration database.</p> <p>Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured.</p> <p>Interacts with the other processes when commands are issued through one of the user interfaces on the switch.</p> <p>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.</p>
Routing protocol process	rpd	<p>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</p>

Related Documentation

Understanding Junos OS with Upgraded FreeBSD

Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. Basing Junos OS on the newer kernel provides Junos OS with sophisticated processing, efficiency, and security features which do not then have to be reproduced in Junos OS.



NOTE: Upgrading to Junos OS Release 15.1 reformats the file system. Only specific files and directories are preserved unless precautions are taken. For details, see [“Upgrading Junos OS with Upgraded FreeBSD” on page 139](#).

Junos OS with an upgraded FreeBSD kernel provides a clean-slate implementation of Junos OS on top of a pristine (minimally modified) and current version of the FreeBSD OS.



NOTE: In Junos OS releases earlier than 15.1, the partition swap pages were counted as part of the memory file system partition. Using this method leaves 4 GB of memory as the maximum that is theoretically accessible when you are using a 32-bit image. However, when Junos OS with upgraded FreeBSD is run, the system only counts the actual partition size, which leaves around 3.4 GB of available physical address space, or only 3 GB of usable RAM. Therefore, we recommend you use a 64-bit image with Junos OS with upgraded FreeBSD.

The platforms currently running Junos OS with upgraded FreeBSD are listed in [Table 4 on page 19](#).

Table 4: Upgraded FreeBSD Kernel Support by Hardware Platform

Platforms	CPU Type	Release Introduced
MX240, MX460, MX960, MX2010, MX2020	Intel	15.1
EX9200	Intel	15.1
QFX5200	Intel	15.1X53-D30
QFX10000 switches	Intel	15.1X53-D60

The major processing changes are as follows:

- Interactions between Junos OS and the upgraded FreeBSD kernel use well-established interfaces because Junos OS is now layered on a minimally modified and current version of FreeBSD.
- Symmetric multiprocessing (SMP) is enabled by default.

- FreeBSD provides a consistent runtime environment for all Junos OS platforms.

There are also major changes in file structures and software packages. These changes are as follows:

- New packages use XML description files instead of scripts.
- Hybrid packages are used to install legacy or replacement build images in the general form **junos-upgrade-x.tgz** where *x* is a variable such as **mx-x86-64-15.1-20150114** (the whole package name is **junos-upgrade-mx-x86-64-15.1-20150114.tgz**).
- Multiple package sets (a collection of installed packages) are stored on the router at the same time. Sets can be either active (the currently used set), pending (the set that should be used at the next reboot), or previous (a formerly active set). Non-recovery snapshots (but not recoverable image snapshots) are available for the package sets to preserve package content lists.

There is now a separate Operations, Administration, and Maintenance (OAM) volume (**oam**) distinct from the Junos OS volume (**junos**). This provides support for downgrades from replacement build images (that is, those using the upgraded FreeBSD kernel) to the legacy Junos OS with a different kernel. The OAM volume allows you to recover the Junos OS volume using recovery snapshots.

One major change is the distinction between recovery snapshots and non-recovery snapshots.

The major characteristics of the recovery snapshots are as follows:

- Recovery snapshots are full copies of the packages and configuration taken at the time the snapshot command is issued.
- Recovery snapshots reside on the OAM volume or USB medium.

The major characteristics of the non-recovery snapshots are as follows:

- Non-recovery snapshots are snapshots residing on the Junos OS volume that refer to the current running set of packages and a copy of the configuration at the time the snapshot command is issued.
- Non-recovery snapshots do not need to copy the whole Junos OS installation and so are very fast.
- Non-recovery snapshots can be requested as the boot image for the next reboot.

The upgraded FreeBSD kernel requires changes to several commands and statements and their related parameters. The new and changed actions are summarized in [Table 5 on page 20](#). For details on the changes, see the topics covering the specific command or statement.

Table 5: New and Changed Commands and Statements for Junos OS with Upgraded FreeBSD

Command or Statement	Release Introduced	Change
<code>request system snapshot delete <i>snapshot</i></code>	15.1	New action

Table 5: New and Changed Commands and Statements for Junos OS with Upgraded FreeBSD (continued)

Command or Statement	Release Introduced	Change
<code>request system snapshot recovery</code>	15.1	New action
<code>request system snapshot load <i>snapshot</i></code>	15.1	New action
<code>request system recover <i>volume</i></code>	15.1	New action: <i>volume</i> is either <code>/junos-volume</code> or <code>/oam-volume</code>
<code>request system snapshot</code>	15.1	Changed action
<code>show system snapshot</code>	15.1	Changed action
<code>request system reboot <i>media</i></code>	15.1	Changed action with new media options

The new FreeBSD kernel also requires that several commands and statements are now deprecated. In some cases, these commands and statements generate an error, and, in other cases, the result is appropriate for the new kernel. The deprecated commands and statements are summarized in [Table 6 on page 21](#). For details, see the topics covering the specific command or statement.

Table 6: Deprecated Commands and Statements for Junos OS with Upgraded FreeBSD

Deprecated Command or Configuration Statement	Release Deprecated
Deprecated Command	
<code>request system partition abort</code>	15.1
<code>request system partition compact-flash</code>	15.1
<code>request system partition hard-disk</code>	15.1
<code>request system snapshot <config-partition></code>	15.1
<code>request system snapshot <root-partition></code>	15.1
<code>request system snapshot <slice></code>	15.1
<code>request system software delete-backup</code>	15.1
<code>request system software rollback <force></code>	15.1
<code>show system processes providers</code>	15.1
<code>show system snapshot <slice></code>	15.1
Deprecated Configuration Statement	

Table 6: Deprecated Commands and Statements for Junos OS with Upgraded FreeBSD (continued)

Deprecated Command or Configuration Statement	Release Deprecated
<code>set system mirror-flash-on-disk</code>	15.1

Related Documentation

- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)
- [Downgrading Junos OS from Upgraded FreeBSD on page 209](#)
- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 327](#)
- [show system snapshot \(Junos OS with Upgraded FreeBSD\) on page 411](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 314](#)

Understanding Junos OS with Upgraded FreeBSD Package Names

Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). In releases earlier than Junos OS Release 15.1, software packages came in several major software package categories, such as domestic, worldwide, or Federal Information Processing Standard (FIPS). However, Junos OS with upgraded FreeBSD has a new naming convention: There is only one category, and FIPS, instead of being a separate category, is an option you select on installation. This topic describes the simplified naming convention for Junos OS with upgraded FreeBSD.

If your hardware platform is listed in the table in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19, then you must use the new package names for download and installation.

The components of the new package naming conventions are as follows:

- **Prefix**—This is **junos-install**. This prefix takes the place of the prefix **jinstall** and the bundle **bundle**. We still use the term *bundle* in the new package-naming convention.
- **Media keyword**—Added to the prefix, a media keyword is only used when the image is not for use with the **request system software add** command. Values for the **media** keyword include **usb** for images installed from a USB drive or **net** for images installed over a network; for example, the entire prefix of your package might be **junos-install-usb-**.
- **Platform**—This field indicates the major product group, such as **mx** or **qfx**.
- **Architecture**—This field indicates the CPU architecture of the platforms. Values include **x86** for Intel and **arm** for Advanced RISC Machines CPUs.
- **Application Binary Interface (ABI)**—This field indicates the “word length” of the CPU architecture. Values include **32** for 32-bit architectures and **64** for 64-bit architectures.
- **Release**—This field indicates the release number, such as **15.1R1.9**.
- **Edition**—The edition field is null (empty) for the standard (domestic) images. For jurisdictions with limits on dataplane encryption, this field is set to **limited**.

As before, all images are in tarred and gzipped (.tgz) format.



NOTE: There are no longer “export” worldwide images or separate FIPS images. The keyword “signed” no longer appears because all Junos OS images are signed for validation.

Examples of valid Junos OS software package names include the following:

- **junos-install-mx-x86-32-15.1R1.9.tgz**—An image for a supported MX Series platform outside the RTZ.
- **junos-install-mx-x86-32-15.1R1.9-limited.tgz**—An image for a supported MX Series platform used in the RTZ.
- **junos-install-usb-mx-x86-32-15.1R1.9.tgz**—An image stored on and installed from a USB drive for a supported MX Series platform outside the RTZ.

Because an upgrade to Junos OS with upgraded FreeBSD from a release earlier than Junos OS 15.1 restructures the disk file system, you can lose many configuration and log files that you might want to keep. Items that are essential can be preserved by moving or copying them to the `/var/preserve` directory.

Related Documentation

- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)

Understanding Junos OS with Upgraded FreeBSD Snapshots

Starting with Junos OS Release 15.1, certain hardware platforms have two types of snapshots. These platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. The two types of snapshots have different content, locations, and purposes, so it is important that they are created and maintained properly. One major change is the distinction between recovery snapshots and non-recovery snapshots. The hardware platforms listed in the table in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19 have these two different types of snapshots.

Recovery snapshots are full copies of the packages and configuration taken at the time the snapshot command is issued. Recovery snapshots reside on the OAM volume or USB medium. Recovery snapshots take some time to complete because of the level of detail captured. Recovery snapshots can be used to recover the Junos OS volume. There is only ever one recovery snapshot on the system.

On the other hand, non-recovery snapshots are snapshots residing on the Junos OS volume that refer to the current running set of packages and a copy of the configuration at the time the snapshot command is issued. Non-recovery snapshots do not need to copy the whole Junos OS installation and so are very fast. They also consume little space, except for the **config.tgz** file. Non-recovery snapshots can be requested as the boot image for the next reboot. You can rename non-recovery snapshots and retain more than one. You rename the non-recovery snapshots with the same procedure used to rename any other file on the system.



NOTE: We recommend that you generate both a non-recovery and a recovery snapshot after you successfully upgrade to Junos OS with upgraded FreeBSD. These snapshots should be refreshed periodically.

Package sets relate to non-recovery and recovery snapshots. The `/active`, `/pending`, and `/previous` sets are all package sets. A non-recovery snapshot is also a package set in a sense, with the addition of a copy of the configuration at the time that the non-recovery snapshot is taken.

Packages that are no longer referenced by any package set or non-recovery snapshot are automatically deleted. We recommend deleting any old non-recovery snapshots after an upgrade so that old packages can be deleted and space recovered.

Some helpful commands for non-recovery snapshots are:

- **request system snapshot**—Use this command to create a non-recovery snapshot.
- **show system snapshot**—Use this command to list all the available non-recovery snapshots.
- **request system snapshot delete**—Use this command to delete a non-recovery snapshot.
- **request system snapshot recovery**—Use this command to create a recovery snapshot. You can use other parameters to determine the details of the recovery snapshot created. There is only ever one recovery snapshot on the system.

Related Documentation

- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 327](#)
- [show system snapshot \(Junos OS with Upgraded FreeBSD\) on page 411](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 314](#)
- [request system software validate on \(Junos OS with Upgraded FreeBSD\) on page 359](#)
- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)
- [Understanding Junos OS with Upgraded FreeBSD Package Names for EX2300 and EX3400 Switches](#)
- [Understanding Junos OS with Upgraded FreeBSD Disk Volumes on page 24](#)

Understanding Junos OS with Upgraded FreeBSD Disk Volumes

Starting with Junos OS Release 15.1, certain hardware platforms have a new disk naming convention. These platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD.

The hardware platforms listed in the table in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19 have two volumes. The main device is the `/junos` volume and contains all of the software and files needed for the day-to-day running of the device. The compact flash drive is the `/oam` volume and stores recovery snapshot backup

information. In case of failure of the main drive (that is, the `/junos` volume), the `/oam` volume can be used to boot the system.

Because the `/junos` and `/oam` volumes have very different purposes, their content is different. Technically, these volumes are `dev/gpt/oam` and `dev/gpt/junos`, but the short forms (`/junos` and `/oam`) are used in this topic. Essentially, the `/junos` volume is used for the running device software and holds configuration information and logs, whereas the `/oam` volume is used for backup copies of everything needed in the event that the `/junos` volume fails.

The `/junos` volume contains a directory named `/packages/db` that has all the components present on the device, such as `os-kernel-123`, `os-kernel-456`, and so on. A sibling directory named `/package-sets` is also present. Package sets are an important concept in Junos OS with upgraded FreeBSD.

The `/package-sets` directory contains a package listing that gathers all the components of the running Junos OS into an XML format in the `/active` subdirectory. So `os-kernel-123` could be a component in the `/package-sets/active` subdirectory, but then `os-kernel-456` could not be in the same XML package. Package sets do not contain the kernel software itself (for example), but tell the device where to find the kernel component needed for the software package. The same kernel can be present in several package listings, but only one package can be active and running on the device at any given time.

There are several directories on the `/junos` volume where a particular software package listing can be found:

- `/previous`—The package set in this directory contains the list of all the components that ran on the device before the last upgrade.
- `/active`—The package set in this directory contains the list of all the software components currently running on the device.
- `/pending`—The package set in this directory contains the list of all the software components on the device that will run after the next reboot.



NOTE: After a successful reboot, the package set in the `/pending` directory becomes the active package set, and the package set in the `/active` directory becomes the previous set.

The `/junos` volume also contains non-recovery snapshots taken with the `request system snapshot` command. These types of snapshots are new to Junos OS with upgraded FreeBSD and cannot be used for recovery of a failed system. Non-recovery snapshots are a special type of package set that includes a copy of the configuration. There can be many non-recovery snapshots on the device, and the files can be renamed. Multiple non-recovery snapshots, essentially lists of software components and configuration files, can be helpful when major software or configuration changes are occurring and establishment of a known stable system baseline is required.

On the other hand, a recovery snapshot, created with the **request system snapshot recovery** command, is stored on the **/oam** volume and is always replaced when a new recovery snapshot is taken.

The **/oam** volume should contain all the information needed to reboot the system if there is a failure of the **/junos** volume and restore the system to the state running at the time of the failure. In order to perform this reboot, the **/oam** volume needs to have all of the information required to provide the system with a running configuration. This information is provided by the recovery snapshot, created with the **request system snapshot recovery** command. Although it can take a while to perform, the recovery snapshot establishes an **.izo** or **.iso** image of the running Junos OS.

In the case of a total failure of the **/junos** volume, the system can be booted from the **/oam** volume. The recovery snapshot can then restore the repaired system.

**Related
Documentation**

- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)

CHAPTER 2

Hardware Overview

- [Hardware Architecture Overview on page 27](#)
- [Hardware Overview \(ACX Series, M Series, MX Series, T Series, and TX Matrix Routers\) on page 28](#)
- [Hardware Overview of SRX Series Services Gateways on page 31](#)
- [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 32](#)
- [Storage Media Names for SRX Series Devices on page 34](#)
- [Boot Sequence on M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series Devices with Routing Engines on page 35](#)
- [Boot Sequence on SRX Series Devices on page 37](#)

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](#).

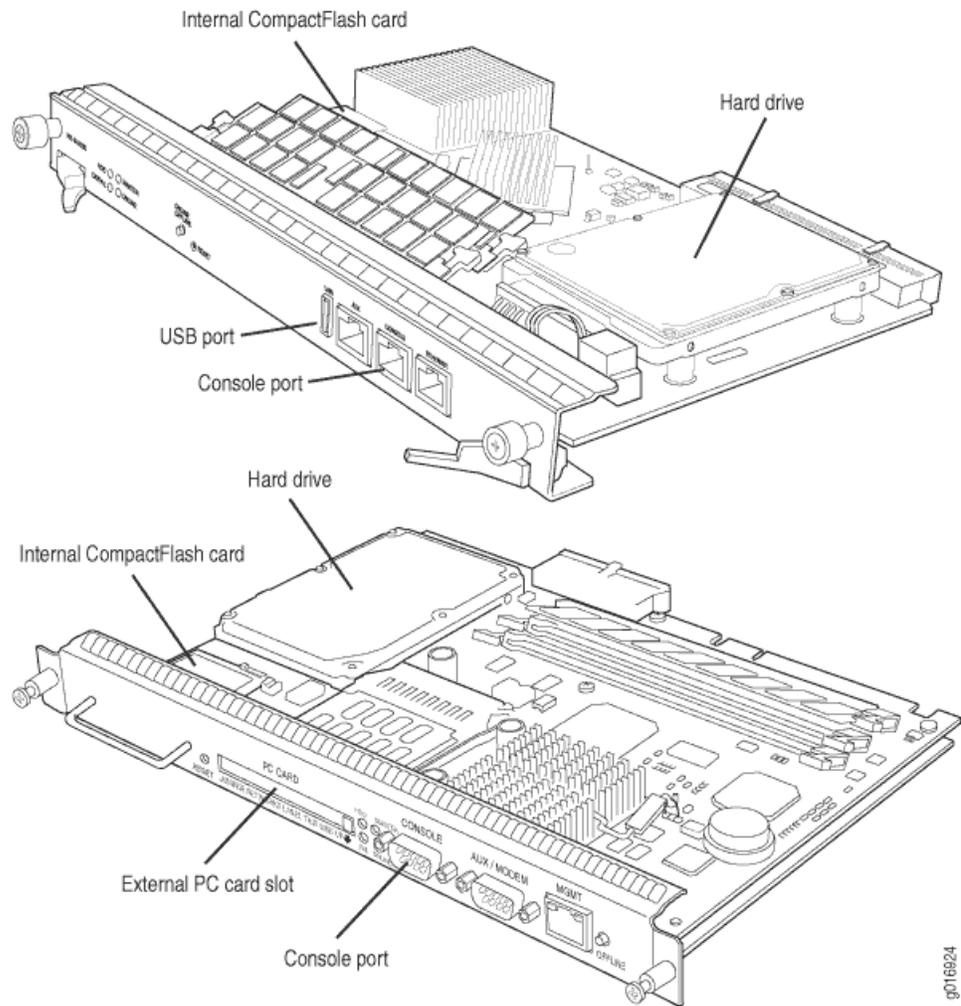
**Related
Documentation**

- [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 29 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 29](#)
- [Storage Media on page 30](#)

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 of SRX Series Services Gateways

SRX Series Device Overview

Figure 3 on page 31 shows the front panel of an SRX345 device.

Figure 3: SRX345 Device Front Panel

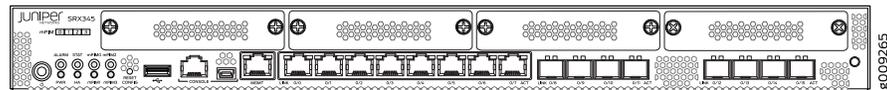


Figure 4 on page 31 shows an example of an SRX1500 device.

Figure 4: SRX1500 Device Front Panel

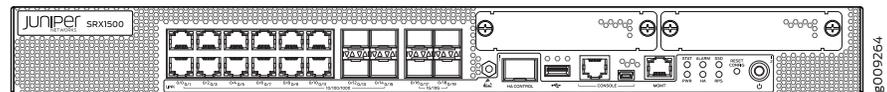


Figure 5 on page 31 shows an example of an SRX5800 device Routing Engine.

Figure 5: SRX5800 Device Routing Engine

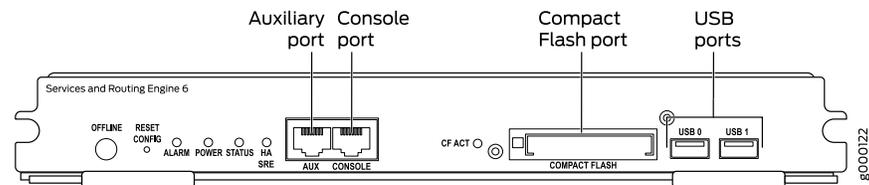
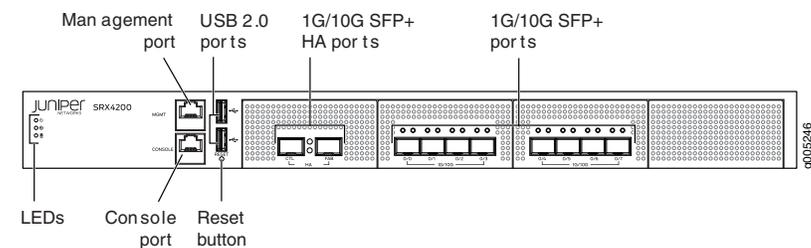


Figure 6 on page 31 shows an example of an SRX4200 device.

Figure 6: SRX4200 Services Gateway Front Panel



System Memory

The amount of free disk space necessary to upgrade a device with a new version of 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 SRX300, SRX320, SRX340, 345 Services Gateway can boot from the following storage media (in the order of priority):

- Internal NAND flash device mounted on the internal eUSB card (default; always present)
- USB storage key (alternate)

The SRX550M Services Gateway can boot from the following storage media (in the order of priority):

- CompactFlash (default; always present)
- USB storage key (alternate)

SRX1500 device use the following media storage devices:

- Internal eSATA flash disk (default; always present)
- SSD card

SRX5400, 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.

The SRX4100 and SRX4200 devices include the following storage media:

- Internal eSATA flash disk (default; always present)
- SSD card

Related Documentation

- [Boot Sequence on SRX Series Devices on page 37](#)
- [Verifying PIC Combinations on page 267](#)

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 7 on page 33 specifies the storage media names by Routing Engine. The storage media device names are displayed when the router boots.

Table 7: 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
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

Table 7: 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-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](#)

Storage Media Names for SRX Series Devices

Table 8 on page 34 specifies the storage media names used by the SRX Series devices. The storage media device names are displayed as the device boots.

Table 8: Storage Media Names

Device	Internal CompactFlash Card	USB Storage Media Devices
SRX Series device	da0	da1

To view the storage media currently available on your system, use the CLI `show system storage` command.

- Related Documentation**
- [Hardware Overview of SRX Series Services Gateways on page 31](#)
 - [Boot Sequence on SRX Series Devices on page 37](#)

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 SRX Series Devices

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

- Internal CompactFlash card
- Internal eSATA flash disk (for SRX1500, SRX4100, and SRX4200 devices)
- USB storage media device

Related Documentation

- [Hardware Overview of SRX Series Services Gateways on page 31](#)
- [Storage Media Names for SRX Series Devices on page 34](#)

PART 2

Installing Junos Software

- [Installation Overview on page 41](#)
- [Performing a Standard or Change Category Installation on page 47](#)
- [Configuring Zero Touch Provisioning on page 73](#)
- [Configuring Automatic Installation of Configuration Files on page 81](#)
- [Configuring Dual-Root Partitions for High Availability on page 95](#)
- [Upgrading Software on page 115](#)
- [Booting a Device Using a System Snapshot on page 159](#)
- [Performing a Recovery Installation on page 165](#)
- [Reinstalling Software on page 187](#)
- [Downgrading Software on page 209](#)
- [Rebooting or Halting Software Processes on a Device on page 213](#)

CHAPTER 3

Installation Overview

- [Installation Type Overview on page 41](#)
- [Installation Categories on the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus Routers on page 42](#)
- [Installation Categories on SRX Series Devices on page 43](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)

Installation Type Overview

The three types of installations used to upgrade or downgrade your routing platform are standard installation, category change, and recovery. 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 information on the different installation packages available, see [“Junos OS Installation Packages” on page 6](#).

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 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.

Related Documentation

- [Junos OS Installation Packages on page 6](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)

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 SRX Series Devices

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

- Junos OS, domestic—`junos-srxsme-<release>-domestic.tgz` for SRX Series devices. .

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.

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.

Related Documentation

- [Installation Type Overview on page 41](#)
- [Software Package Information Security on page 11](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)

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 on page 44](#)
- [Software Package Security on page 44](#)
- [Installing Software on a Virtual Chassis on page 45](#)
- [Installing Software on Switches with Redundant Routing Engines on page 45](#)
- [Installing Software Using Automatic Software Download on page 45](#)
- [Autoinstalling a Configuration File on an EX2200 or EX3300 Switch from a Disk-on-Key USB Memory Stick on page 46](#)
- [Installing Software on an EX2300 or EX3400 Switch on page 46](#)
- [Troubleshooting Software Installation on page 46](#)

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 follow 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 123](#). 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)*.

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 129.

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.

Installing Software on an EX2300 or EX3400 Switch

Before installing software on an EX2300 or EX3400 switch:

- Ensure that at least 620 MB of disk space is available in the system before downloading the software installation package to the `/var/tmp` directory. Use the command `show system storage` to get details of the available space.
- If the space available is inadequate, use the command `request system storage cleanup`. Additionally, you can manually delete any other log or unwanted files from the `/var/tmp` or `/var/log` directories.

You can now follow the procedure in *Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)* to complete the software installation.

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 263.



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 51](#)
- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Installing Software on an EX Series Switch with a Single Routing Engine \(CLI Procedure\)](#)
- [Installing Software on an EX Series Switch with Redundant Routing Engines \(CLI Procedure\)](#)
- [Understanding Nonstop Software Upgrade on EX Series Switches on page 123](#)

CHAPTER 4

Performing a Standard or Change Category Installation

- [Checking the Current Configuration and Candidate Software Compatibility on page 47](#)
- [Determining the Junos OS Version on page 48](#)
- [Downloading Software on page 48](#)
- [Downloading Software Packages from Juniper Networks on page 51](#)
- [Understanding Download Manager for SRX Series Devices on page 51](#)
- [Understanding the Console Port on page 53](#)
- [Backing Up the Existing Installation on Routers on page 55](#)
- [Backing Up the Current Installation on SRX Series Devices on page 56](#)
- [Installing the Software Package on a Router with a Single Routing Engine on page 57](#)
- [Installing the Software Package on a Router with Redundant Routing Engines on page 58](#)
- [Repartitioning Routing Engine System Storage To Increase the Swap Partition on page 64](#)
- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Registering the EX Series Switch with the J-Web Interface on page 66](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 66](#)
- [Installing Junos OS on SRX Series Devices Using a USB Flash Drive on page 68](#)
- [Upgrading the Boot Loader on SRX Series Devices on page 69](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 70](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 72](#)

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

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 153](#)
- [request system snapshot \(SRX Series\) on page 329](#)
- [request system software add \(Maintenance\) on page 342](#)

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.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 153](#)

Downloading Software

You can download the software in one of two ways:

- [Downloading Software with a Browser on page 49](#)
- [Downloading Software Using the Command-Line Interface on page 49](#)

Downloading Software with a Browser

You download the software package you need from the Juniper Networks Support website 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 website: <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 website 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 website: <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
```

Related Documentation

- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)

- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 153](#)

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 for EX Series Switches](#)” on page 7.
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 \(CLI Procedure\)](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)

Understanding Download Manager for SRX Series Devices

This topic includes the following sections:

- [Overview on page 51](#)
- [Using Download Manager to Upgrade Junos OS on page 52](#)
- [Handling Errors on page 52](#)
- [Considerations on page 53](#)

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 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 9 on page 53](#) 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 9: 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

- [Installation Type Overview on page 41](#)

Understanding the Console Port

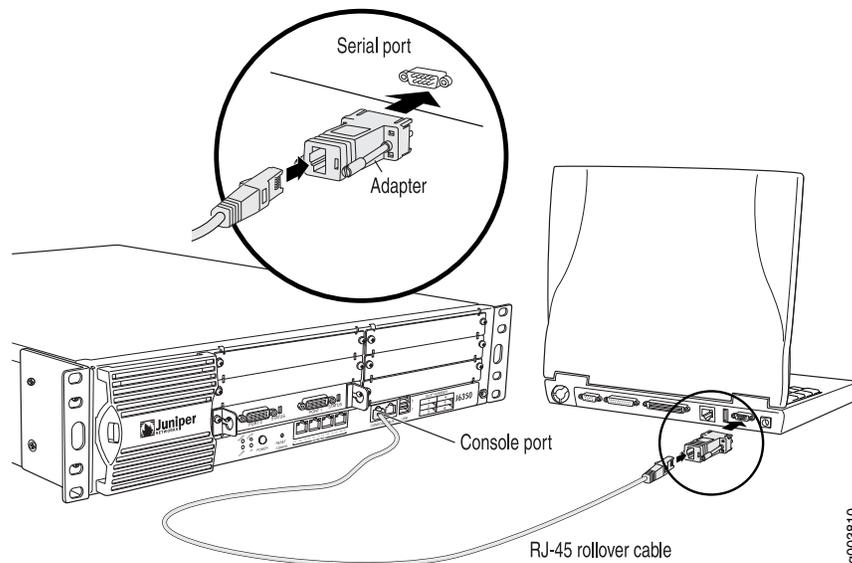
Console ports allow root access to the Junos operating system (Junos OS) devices through a terminal or laptop interface, regardless of the state of the Junos OS device,

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 54](#).

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



Related Documentation

- *Accessing a Junos OS Device the First Time*

g0038110

Backing Up the Existing Installation on Routers

The installation process removes some files stored on the router. In the case of Junos OS, all stored files except the **juniper.conf** and SSH files are removed. Therefore, you must back up your existing installation in case you need to return to it. This topic describes how to back up the existing Junos OS installation on routers.

As of Junos OS Release 15.1, certain platforms run Junos OS based on an upgraded FreeBSD kernel (Junos OS with upgraded FreeBSD). For information about backing up Junos OS with upgraded FreeBSD, see [“Upgrading Junos OS with Upgraded FreeBSD” on page 139](#). For the platforms using Junos OS with upgraded FreeBSD, see [“Understanding Junos OS with Upgraded FreeBSD” on page 19](#).

For information about backing up the existing installation on SRX Series Services Gateways, see [“Backing Up the Current Installation on SRX Series Devices” on page 56](#).

On routers, you should back up the current installation so that you can return to it if needed.

In a dual Routing Engine system, you need to back up both Routing Engines.

To back up files to the router’s hard disk or solid-state drive (SSD):

- Issue the **request system snapshot** CLI operational command.

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

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 SSD. When the backup is completed, the current and backup software installations are identical.



NOTE: 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.

To back up files on an MX104 to a specified external storage media device:

- Issue the **request system snapshot media** CLI operational command. For example:

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

On MX104 routers, when you issue the **request system snapshot** operational command to back up the current software installation, the backup is done on the first USB storage media device.

To back up files to the router's NAND flash device on ACX Series routers:

- Issue the **request system snapshot slice alternate** CLI operational command.

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

When this command is issued, the **/root** file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig** on the router's NAND flash device.

To back up files from the NAND flash device to a USB storage media device:

- Issue the **request system snapshot** CLI operational command.

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

When you issue the **request system snapshot** operational command to back up the NAND flash device, the backup is done on the first USB storage media device.

**Related
Documentation**

- [request system snapshot on page 320](#)
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)
- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)
- [Backing Up the Current Installation on SRX Series Devices on page 56](#)

Backing Up the Current Installation on SRX Series Devices

This topic includes the following sections:

- [Backing Up the Current Installation on High-End SRX Series Devices on page 56](#)
- [Backing Up the Current Installation on Branch SRX Series Devices on page 57](#)

Backing Up the Current Installation on High-End SRX Series Devices

Back up the current installation so that you can return to the current software installation. The installation process using the installation package (`jinstall*`, for example) removes all stored files on the device 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 SRX Series devices, issue the `request system snapshot` CLI operational command. This command saves the current software installation on the hard disk, external USB storage media device, or solid-state drive (SSD).

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 device's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the device's hard disk or solid-state drive (SSD). When the backup is completed, the current and backup software installations are identical.

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

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

Backing Up the Current Installation on Branch 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.

To back up the currently running and active file system partitions on the device, use the following command:

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

Following options are supported:

- **internal**— Copies the snapshot to internal media.
- **usb**— Copies the snapshot to the USB storage device. This is the default option for Branch SRX Series devices.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 70](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 72](#)

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 48](#).

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 14](#).

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 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 59](#)
2. [Installing Software on the Backup Routing Engine on page 59](#)
3. [Installing Software on the Master Routing Engine on page 61](#)
4. [Finalizing the Installation on page 63](#)

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 48.

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 14.

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 48](#).

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 14](#).

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)
Routing 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](#)

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 57](#)
- [Installing the Software Package on a Router with Redundant Routing Engines on page 58](#)

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 51.
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 10 on page 65](#).
5. Click **Fetch and Install Package**. The software is activated after the switch has rebooted.

Table 10: 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: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i>
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 11 on page 66](#).
4. Click **Upload and Install Package**. The software is activated after the switching platform completes the installation procedure.

Table 11: 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 \(CLI Procedure\)](#)
 - [Understanding Software Installation on EX Series Switches on page 44](#)
 - [Troubleshooting Software Installation on page 263](#)

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](#)

Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series 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.

All USB flash drives used on SRX Series devices must have the following features:

- USB 2.0 or later.
- Formatted with a FAT/FAT 32 or MS-DOS file system



NOTE: The Junos OS package on a USB device is commonly stored in the root drive as the only file; for example, `junos-srxsme-15.1X49-D30.3-domestic.tgz`.



CAUTION: Any USB memory product not listed as supported for SRX Series devices has not been tested by Juniper Networks. The use of any unsupported USB memory product could expose your SRX Series device to unpredictable behavior. Juniper Networks Technical Assistance Center (JTAC) can provide only limited support for issues related to unsupported hardware. We strongly recommend that you use only supported USB flash drives.



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.

- (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 host-1;
  domain-name example.net;
  domain-search [ abc.exmaple.net example.net device1.example.net];
  root-authentication {
    encrypted-password "$ABC123"; ## 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 SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 153](#)

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

To install the Junos OS image on an SRX Series device using a USB flash drive:

- Insert the USB flash drive into the USB port of the SRX Series device and wait for the LEDs to blink amber indicating that the SRX Series device detects the Junos OS image.
If the LEDs do not change to amber, press the Power button or turn the device off and then on again and wait for the LEDs to blink amber.
- Press the **Reset Config** button on the SRX Series device to start the installation and wait for the LEDs to glow steadily amber.

When the LEDs glow green, the Junos OS upgrade image has been 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.

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 SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 153](#)

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

You can install Junos OS using the Trivial File Transfer Protocol (TFTP) method. The device is shipped with Junos OS loaded on the primary boot device. During 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 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 12 on page 71](#).

Table 12: 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.

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 must 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 a 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.
6. Remove the USB flash drive.

Configuring Zero Touch Provisioning

- [Understanding Zero Touch Provisioning on page 73](#)
- [Configuring Zero Touch Provisioning on page 76](#)

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 95](#).



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 76](#)

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 73](#)
- *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 185](#)

CHAPTER 6

Configuring Automatic Installation of Configuration Files

- [Autoinstallation Overview on page 81](#)
- [Example: Configuring Autoinstallation on SRX Series Devices on page 84](#)
- [Configuring Autoinstallation on JNU Satellite Devices on page 87](#)
- [Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89](#)
- [Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91](#)
- [Verifying Autoinstallation on JNU Satellite Devices on page 92](#)

Autoinstallation Overview

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.

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.

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.

This section contains the following topics:

- [Automatic Installation of Configuration Files on page 82](#)
- [Supported Autoinstallation Interfaces and Protocols on page 82](#)
- [Typical Autoinstallation Process on a New Device on page 83](#)

Automatic Installation of Configuration Files

On SRX Series devices, you can specify a remote server where configuration files are located. If a configuration file cannot be found on the device's CompactFlash card, the device 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 device 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
```

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 13 on page 82](#) lists the protocols that the device can use on these interfaces for IP address acquisition.

Table 13: 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)

Table 13: Interfaces and Protocols for IP Address Acquisition During Autoinstallation (*continued*)

Interface and Encapsulation Type	Protocol for Autoinstallation
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 SRX Series Devices on page 84](#)

Example: Configuring Autoinstallation on SRX Series Devices

This example shows how to configure a device for autoinstallation.

- [Requirements on page 84](#)
- [Overview on page 85](#)
- [Configuration on page 85](#)
- [Verification on page 86](#)

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.
- Create one of the following configuration files, and store it on a TFTP server in the network (see [“Configuration Files” on page 15](#)):

- 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 section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system autoinstallation configuration-servers tftp://tftpconfig.sp.com
set system 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*.

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 tftp://tftpconfig.sp.com
```



NOTE: You can also use an FTP address, for example, `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, delete the factory default for that interface. 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 is logged in the message file: “DCD_CONFIG_WRITE_FAILED failed.”

Verification

Confirm that the configuration is working properly.

- [Verifying Autoinstallation on page 86](#)

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 on page 81](#)

Configuring Autoinstallation on JNU Satellite Devices

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. In this scenario, satellite devices, such as EX Series Ethernet Switches, QFX Series devices, and ACX Series Universal Access Routers, that are managed by the controller are considered.

To configure autoinstallation:

1. Load the JNU factory-default configuration file on the satellite device to enable the device to function in JNU mode.

```
user@satellite# load override /etc/config/jnu-factory.conf
```

An override operation discards the current candidate configuration and loads the configuration in the specified filename or the one that you type at the terminal. When you use the override option and commit the configuration, all system processes reparse the configuration.

2. Specify the URL address of one or more servers from which to obtain configuration files.

```
[edit system]
user@host# set autoinstallation configuration-servers tftp://tftpconfig.sp.com
```



NOTE: You can also use an HTTP or FTP address—for example, `http://user:password@httpconfig.sp.com` or `ftp://user:password@sftpconfig.sp.com`.

3. Configure one or more Ethernet interfaces to perform autoinstallation and IP address acquisition protocols for each interface. The router uses the protocols to send a request for an IP address for the interface:

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

4. Set the root password, entering a clear-text password that the system will encrypt, a password that is already encrypted, or an SSH public key string.

Choose one of the following:

- To enter a clear-text password, use the following command:

```
[edit system]
```

```

user@host# set root-authentication plain-text-password
New password: type password here
Retype new password: retype password here

```

- To enter a password that is already encrypted, use the following command:

```

[edit]
root# set system root-authentication encrypted-password encrypted-password

```

- To enter an SSH public key, use the following command:

```

[edit]
root# set system root-authentication ssh-rsa key

```

5. Save the Junos OS configuration changes, activate the configuration on the device and exit configuration mode, using the **commit-and-quit** command.

```

[edit]
user@host# commit-and-quit

```

When the satellite device reboots, it triggers the autoinstallation mechanism to retrieve its initial configuration and downloads the settings from the configuration file stored on a configuration server in the network. On the controller, you must enable the FTP service by using the **set system services ftp** command and save the configuration on the satellite device at the `/var/jnu/` directory.

The following configuration is generated on the satellite device as a result of the preceding procedure to configure autoinstallation:

```

system {
  autoinstallation {
    traceoptions {
      flags {
        all;
      }
      file autod;
      level all;
    }
    delete-after-commit; /* After initial config, no need to keep */
    interfaces {
      ge-* {
        bootp;
      }
      xe-* {
        bootp;
      }
      configuration-servers {
        "ftp://192.168.0.1/var/jnu/sat1.conf";
      }
    }
  }
  root-authentication {
    encrypted-password "$ABC123";
  }
}

```

- Related Documentation**
- [Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91](#)
 - [Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89](#)
 - [Verifying Autoinstallation on JNU Satellite Devices on page 92](#)
 - [autoinstallation on page 278](#)
 - [delete-after-commit \(JNU Satellites\) on page 282](#)
 - [configuration-servers](#)

Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group

Autoinstallation provides automatic configuration for a new router that you connect to the network and power 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 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 CompactFlash card. The autoinstallation feature enables you to deploy multiple routers 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 router.

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

This topic describes:

- [Supported Autoinstallation Interfaces and Protocols on page 89](#)
- [Typical Autoinstallation Process on a New Router on page 90](#)

Supported Autoinstallation Interfaces and Protocols

Before autoinstallation on a router can take place, the router must acquire an IP address or a USB key. The protocol or protocols you choose for IP address acquisition determine the router interface to connect to the network for autoinstallation. The router detects the connected interface and requests an IP address with a protocol appropriate for the interface. Autoinstallation is supported over an Ethernet LAN interface. For IP address acquisition, the JNU satellite router uses DHCP, BOOTP, or Reverse Address Resolution Protocol (RARP) on an Ethernet LAN interface.

If the server with the autoinstallation configuration file is not on the same LAN segment as the new router, or if a specific router is required by the network, you must configure an intermediate router directly attached to the new router, through which the new router can send HTTP, FTP, Trivial File Transfer Protocol (TFTP), BOOTP, and Domain Name

System (DNS) requests. In this case, you specify the IP address of the intermediate router as the location to receive HTTP, FTP, or TFTP requests for autoinstallation.

Typical Autoinstallation Process on a New Router

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

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

If a DHCP server responds, it provides the router 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 HTTP, FTP, or TFTP server.
- The IP address or hostname of the HTTP, FTP, or 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 router if the configuration server is on a different LAN segment from the new router.
2. After the new router acquires an IP address, the autoinstallation process on the router attempts to download a configuration file in the following ways:
 - a. If the configuration file is specified as a URL, the router fetches the configuration file from the URL by using HTTP, FTP, or TFTP depending on the protocol specified in the URL.
 - b. If the DHCP server specifies the host-specific configuration file (boot file) **hostname.conf**, the router uses that filename in the TFTP server request. (In the filename, **hostname** is the hostname of the new router.) The autoinstallation process on the new router makes three unicast TFTP requests for **hostname.conf**. If these attempts fail, the router broadcasts three requests to any available TFTP server for the file.
 - c. If the new router cannot locate **hostname.conf**, the autoinstallation process unicasts or broadcasts TFTP requests for a default router configuration file called **network.conf**, which contains hostname-to-IP address mapping information, to attempt to find its hostname.
 - d. If **network.conf** contains no hostname entry for the new router, the autoinstallation process sends out a DNS request and attempts to resolve the new router's IP address to a hostname.

- e. If the new router can determine its hostname, it sends a TFTP request for the *hostname.conf* file.
 - f. If the new router 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 router locates a configuration file on a TFTP server, the autoinstallation process downloads the file, installs the file on the router, and commits the configuration.

Related Documentation

- [Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91](#)
- [Configuring Autoinstallation on JNU Satellite Devices on page 87](#)
- [Verifying Autoinstallation on JNU Satellite Devices on page 92](#)
- [autoinstallation on page 278](#)
- [delete-after-commit \(JNU Satellites\) on page 282](#)
- [configuration-servers](#)

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 on page 89](#)
- [Configuring Autoinstallation on JNU Satellite Devices on page 87](#)
- [Verifying Autoinstallation on JNU Satellite Devices on page 92](#)
- [autoinstallation on page 278](#)
- [delete-after-commit \(JNU Satellites\) on page 282](#)
- [configuration-servers](#)

Verifying Autoinstallation on JNU Satellite Devices

Purpose After you have configured autoinstallation, display the status of autoinstallation on a satellite device, such as an ACX Series router, an EX Series switch, or a QFX Series device, in a Junos Node Unifier (JNU) group that is managed by a controller, which is an MX Series router.

Action From the CLI, enter the **show system autoinstallation status** command. The following example displays the autoinstallation settings of an ACX Series router that operates as a satellite in a JNU group.

Sample Output

```
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-0/1/0
  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: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
Interface:
  Name: ge-0/1/1
  State: None
  Address acquisition:
    Protocol: DHCP Client
    Acquired address: None
    Protocol: RARP Client
```

Acquired address: None

Meaning The output shows the settings configured for autoinstallation. Verify that the values displayed are correct for the router when it is deployed on the network.

- Related Documentation**
- [Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91](#)
 - [Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89](#)
 - [Configuring Autoinstallation on JNU Satellite Devices on page 87](#)
 - [autoinstallation on page 278](#)
 - [delete-after-commit \(JNU Satellites\) on page 282](#)
 - [configuration-servers](#)
 - [show system autoinstallation status on page 381](#)

CHAPTER 7

Configuring Dual-Root Partitions for High Availability

- [Understanding Resilient Dual-Root Partitions on Switches on page 95](#)
- [Resilient Dual-Root Partitions Frequently Asked Questions on page 99](#)
- [Dual-Root Partitioning Scheme on SRX Series Devices on page 105](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110](#)

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 \(Junos OS Release 10.4R3 and Later\) on page 96](#)
- [Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature on page 96](#)

- [Earlier Partition Scheme \(Junos OS Release 10.4R2 and Earlier\)](#) on page 97
- [Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases](#) on page 98

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 14 on page 96](#).

Table 14: Resilient Dual-Root Partition Scheme

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

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 15 on page 98](#).

Table 15: Earlier Partition Scheme

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

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 14 on page 96](#).

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 99](#)

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? on page 99](#)
- [What Happens If I Do Not Upgrade Both the Loader Software and Junos OS at the Same Time? on page 100](#)
- [Can I Downgrade Junos OS Without Downgrading the Loader Software? on page 101](#)
- [Can I Upgrade to a Resilient Dual-Root Partition Release by Using the CLI? on page 101](#)
- [Will I Lose My Configuration During an Upgrade? on page 102](#)
- [How Long Will the Upgrade Process Take? on page 102](#)
- [What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Enabled? on page 102](#)
- [What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Not Enabled? on page 103](#)
- [How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System? on page 103](#)
- [Can I Use Automatic Software Update and Download to Upgrade to a Resilient Dual-Root Partition Release? on page 104](#)
- [Why Is the Message "At least one package installed on this device has limited support" Displayed When Users Log In to a Switch? on page 104](#)
- [Where Can I Find Instructions for Upgrading? on page 104](#)

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	<p>New loader software</p> <p>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.)</p> <p>For EX8200 switches: U-Boot 1.1.6 (Jan 11 2008 - 05:24:35) 3.5.0 (Contains version 3.5.0.)</p>	Recommended
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.

Table 16: Combinations of Junos OS Versions and Loader Software Versions (*continued*)

Junos OS Release	Loader Software	Notes
Release 10.4R3 and later	<p>Old loader software</p> <p>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)</p> <p>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.)</p>	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	<p>New loader software</p> <p>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.</p>	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 102](#) 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
/	/	/var	/var/tmp	/config
(root Junos OS)	(root Junos OS)			
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.		
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 103 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
/	/	/var	/var/tmp	/config
(root Junos OS)	(root Junos OS)			
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 131](#)

- [Troubleshooting Software Installation on page 263](#)
- [Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 266](#)
- [Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 131](#)

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.



NOTE: Junos OS Release 12.1X45 and later do not support single root partitioning.

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 SRX Series Devices on page 106](#)
- [Important Features of the Dual-Root Partitioning Scheme on page 106](#)
- [Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning on page 106](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers Devices on page 108](#)
- [Understanding How Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on page 109](#)

Boot Media and Boot Partition on 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 19 on page 106 provides information on the storage media available on SRX Series devices.

Table 19: Storage Media on SRX Series Devices

SRX Series Devices	Storage Media
SRX300, SRX320, and SRX340, and SRX345	<ul style="list-style-type: none"> eUSB disk (default; always present) USB storage device (alternate)
SRX550M	<ul style="list-style-type: none"> Internal CF (default; always present) USB storage device (alternate)

With the dual-root partitioning scheme, the SRX Series device first tries to boot 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 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.

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.

```
*****
**
**  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 and if auto-snapshot feature is not     **
**  enabled.                                                       **
**                                                              **
*****
```

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.



NOTE: We recommend performing the snapshot once all the processes start. This is done to avoid any increase in the reboot time.



NOTE:

- Auto-snapshot feature is supported on branch SRX Series devices.
- By default the auto-snapshot feature is disabled.
- If you do not maintain the same version of Junos OS in both partitions, ensure that the automatic snapshot feature remains disabled. Otherwise, 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.

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 must 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 alternate** to back up the currently running root file system (primary or secondary) to the other root partition on the system along with following:

- 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 How 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 from the Boot Loader Using a TFTP Server” on page 70](#)
- 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 from the Boot Loader Using a USB Storage Device” on page 72](#)
- 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 SRX Series Devices on page 145](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110](#)

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 on page 110](#)
- [Overview on page 110](#)
- [Configuration on page 111](#)
- [Verification on page 113](#)

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 must back up any important data before starting the process.



NOTE: Partition install is supported on the default media on SRX300, SRX320, 340, and SRX345 devices (internal NAND flash) and *not* supported on the alternate media (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 must 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 install Junos OS Release 10.0 or later with the `partition` option, enter the following command from operational mode:

```
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 to Upgrade Junos OS on SRX Series Devices”](#) on page 66.
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 113](#)

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 105](#)

CHAPTER 8

Upgrading Software

- [Upgrading Software Packages on page 116](#)
- [Upgrading to 64-bit Junos OS on page 119](#)
- [Upgrading Routers Using Unified ISSU on page 122](#)
- [Understanding Nonstop Software Upgrade on EX Series Switches on page 123](#)
- [Upgrading Software by Using Automatic Software Download on page 129](#)
- [Verifying That Automatic Software Download Is Working Correctly on page 131](#)
- [Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 131](#)
- [Upgrading the Loader Software on the Line Cards in a Standalone EX8200 Switch or an EX8200 Virtual Chassis on page 136](#)
- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 153](#)
- [Understanding BIOS Upgrades on SRX Series Devices on page 154](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 156](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 156](#)

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 `bundle` 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.)



NOTE: If you are upgrading a Routing Engine on a PTX Series router to run Junos OS Release 13.2R2 and later, and then make that Routing Engine the master Routing Engine, then the master Routing Engine reports a major alarm `CB 0/1 ESW PFE Port Fail` even though the Control Board's Ethernet switch links are up and running on both the master and the backup Routing Engines. This is because the backup Routing Engine is still on Junos OS Release 13.2R1 or earlier. The alarm is cleared after you have completed the upgrade of Junos OS on the backup Routing Engine.

```
User@router# show chassis alarms
2 alarms currently active
Alarm time Class Description
2014-10-15 00:44:31 BST Major CB 0 ESW PFE Port Fail
2014-10-15 00:42:42 BST Minor Backup RE Active
```

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 48.



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.



NOTE: High-end SRX Series devices, 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: This step is optional for branch SRX Series devices. For branch SRX Series devices, ensure that a USB flash drive is plugged into the USB port of the device.

- 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
```

- 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.



NOTE: For high-end SRX Series devices, 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 is the same. In such cases, the package gets deleted after a successful upgrade.

If you are upgrading more than one package at the same time, add `jbases` 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 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*.

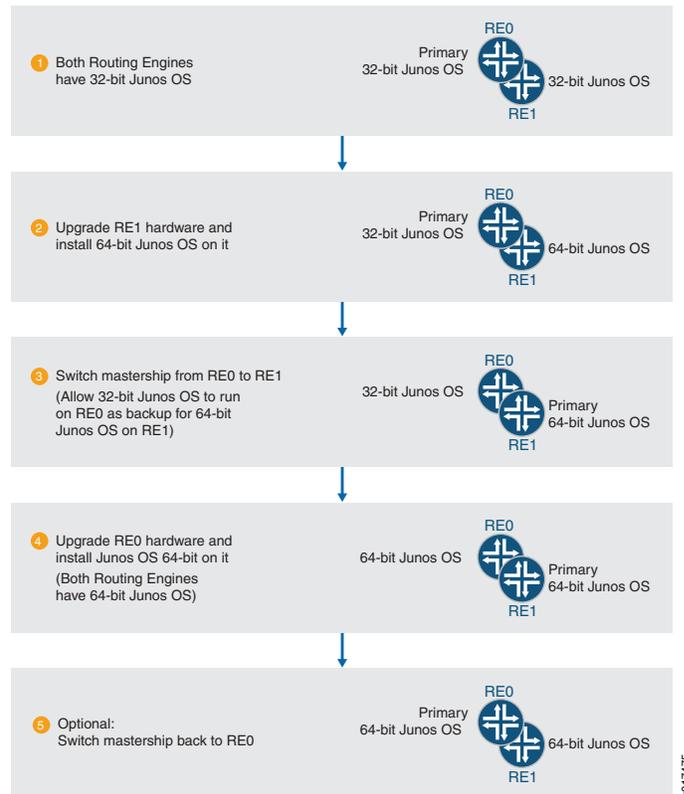
Before you begin, you must have:

- 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 120](#) and perform the following steps:

Figure 8: Upgrading to the 64-bit Junos OS with Dual Routing Engines

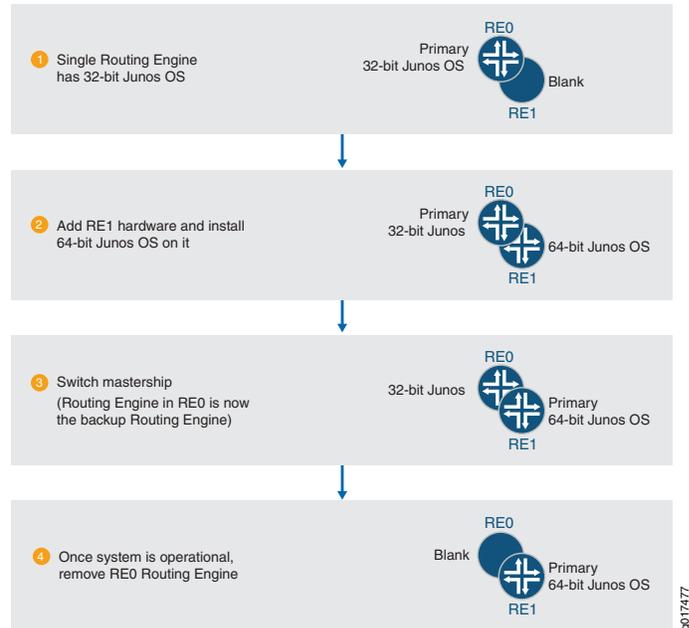


1. In the initial state, both Routing Engines are running the 32-bit Junos OS, and slot 0 has the master Routing Engine.
2. Upgrade the slot 1 Routing Engine hardware and install the 64-bit Junos OS.
For instructions on replacing a Routing Engine, see the hardware guide for your router.
3. Switch the 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)

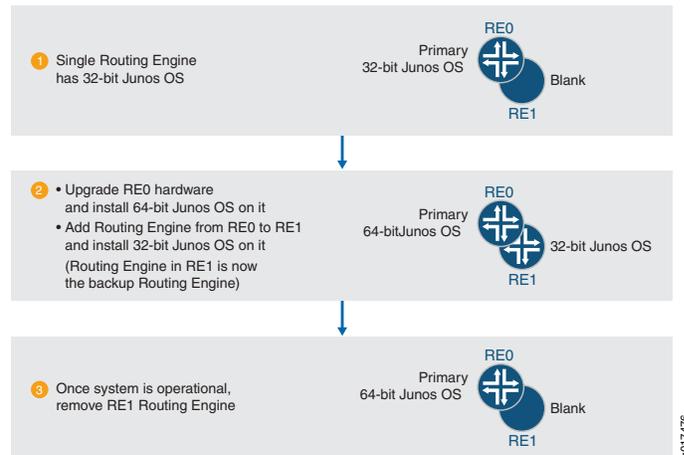


To upgrade a system with a single Routing Engine, where the master Routing Engine can be in either slot 0 or slot 1, refer to [Figure 8 on page 120](#) and perform the following steps:

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 122](#) 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 187](#)

Upgrading Routers Using Unified 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. Unified 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 unified ISSU, see the *Junos OS High Availability Library for Routing Devices*.

For additional information about using unified ISSU on SRX Series devices, see the [Junos OS Chassis Cluster Library for Security Devices](#).

Related Documentation

- [Upgrading Individual Software Packages on page 116](#)

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)*.

This topic covers:

- [Requirements for Performing an NSSU on page 124](#)
- [How an NSSU Works on page 125](#)
- [NSSU Limitations on page 128](#)
- [NSSU and Junos OS Release Support on page 128](#)
- [Overview of NSSU Configuration and Operation on page 129](#)

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 125](#)
- [EX6200 and EX8200 Switches on page 126](#)
- [EX8200 Virtual Chassis on page 127](#)

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 20 on page 128](#) lists the EX Series switches and Virtual Chassis that support NSSU and the Junos OS release at which they began supporting it.

Table 20: 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 20: 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 124. 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*.

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)*
- *Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)*
- *Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)*
- *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*

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 131](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)
- [Configuring DHCP Services \(J-Web Procedure\)](#)

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 129](#)

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 on page 132](#)
- [Verifying the Loader Software Version on page 132](#)
- [Verifying Which Root Partition Is Active on page 133](#)
- [Verifying the Junos OS Version in Each Root Partition on page 134](#)

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 263](#)
 - [Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 266](#)
 - [Understanding Resilient Dual-Root Partitions on Switches on page 95](#)
 - [Resilient Dual-Root Partitions Frequently Asked Questions on page 99](#)

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-8200-11.3build-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
FPC 7               U-Boot              0  2.3.0
Routing Engine 0 RE BIOS  0  3.1.1
Routing Engine 1    0  3.1.1
                   OK
                   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 version	Available version	Status
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.

- 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.

- 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)*
- Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)*
- Troubleshooting an EX8200 Line Card's Failure to Power On*

Upgrading Junos OS with Upgraded FreeBSD

Starting with Junos OS Release 15.1, certain hardware platforms run an upgraded FreeBSD kernel instead of older versions of FreeBSD.

Before you begin:

- Verify that the upgrade applies to your router or switch model, as listed in [“Understanding Junos OS with Upgraded FreeBSD” on page 19](#).
- Download the Junos OS package.
- Determine the upgrade path to follow.

The current Junos OS release determines the upgrade path to Junos OS with upgraded FreeBSD, as shown in [Table 21 on page 139](#). Other upgrade paths might work, but they are not supported.

Table 21: Upgrade Path to Junos OS with the Upgraded FreeBSD

Current Router's Junos OS Release	Upgrade Path
12.3 or earlier	Upgrade to 13.3. or 14.2 first, then upgrade to 15.1 or later (multiple steps).

Table 21: Upgrade Path to Junos OS with the Upgraded FreeBSD (continued)

Current Router's Junos OS Release	Upgrade Path
13.3 or later	Use upgrade package to upgrade from the current Junos OS release to Junos OS with upgraded FreeBSD (single step).
15.1 or later	Use upgrade package to upgrade from the current Junos OS release to Junos OS with upgraded FreeBSD (single step).



NOTE: You can also downgrade from Junos OS Release 15.1 to an earlier release of Junos OS, as long as the path complies with the Junos OS policy of skipping at most two releases earlier.

- Understand that direct validation of running configuration does not work for upgrading to Junos OS with upgraded FreeBSD from Junos OS based on older versions of the FreeBSD kernel.

When upgrading or downgrading between Junos OS and Junos OS with upgraded FreeBSD, you might have to validate on a different host. It does not matter where that other host is, as long as you can reach it with NETCONF over SSH. See *Establishing an SSH Connection for a NETCONF Session*. The target system uses the network to contact the other host, run the validation and authentication, and return the result.

The upgrade process only preserves the following directories:

- /config
- /etc/localtime
- /var/db
- /var/etc/master.passwd
- /var/etc/inetd.conf
- /var/etc/pam.conf
- /var/etc/resolv.conf
- /var/etc/syslog.conf
- /var/etc/localtime
- /var/etc/exports
- /var/etc/extensions.allow
- /var/preserve
- /var/tmp/baseline-config.conf
- /var/tmp/preinstall_boot_loader.conf



NOTE: On EX2300 and EX3400 switches, the following directories are not applicable:

- /etc/localtime
- /var/etc/localtime
- /var/etc/exports
- /var/preserve
- /var/tmp/preinstall_boot_loader.conf

For specific installation procedures, see the following:

- [To Install Junos OS with Upgraded FreeBSD Over a Plain Junos OS on page 141](#)
- [To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of an Earlier Release on page 144](#)
- [To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of a Later Release on page 145](#)

To Install Junos OS with Upgraded FreeBSD Over a Plain Junos OS



NOTE: If you have important files in other directories, copy them from the router or switch to a secure location before upgrading the router or switch.



NOTE: The following procedure refers to routers, but it also applies to switches.

To install Junos OS with upgraded FreeBSD over a plain Junos OS:

1. Enter the `request system software add package-name no-validate` command from the operational mode in the CLI:



NOTE: The `no-copy` option is enabled by default.

Use the `no-validate` option with the `request system software add` command. If you leave out the `no-validate` option, the command uses the `validate` option by default, and direct validation of running configuration does not work for upgrading to Junos OS with upgraded FreeBSD from Junos OS based on older versions of the FreeBSD kernel.



NOTE: You can also use `reboot` option along with `request system software add` command, but it is not recommended to do this in a single step while upgrading from a FreeBSD 6.1 based Junos OS to FreeBSD 10 based Junos OS.



NOTE: To validate current configuration on an upgrade to Junos OS with upgraded FreeBSD from Junos OS, use the `request system software validate on (Junos OS with Upgraded FreeBSD)` command.

```
user@host>request system software add
/var/tmp/junos-install-mx-x86-32-15.1R1.9.tgz no-validate
Installing package '/var/tmp/junos-install-mx-x86-32-15.1R1.9.tgz' ...
Verified manifest signed by PackageProductionEc_2015
Verified manifest signed by PackageProductionRSA_2015
Verified contents.iso
Verified issu-indb.tgz
Verified junos-x86-32.tgz
Verified kernel
Verified metatags
Verified package.xml
Verified pkgtools.tgz
camcontrol: not found
camcontrol: not found
Verified manifest signed by PackageProductionEc_2015
Saving the config files ...
NOTICE: uncommitted changes have been saved in
/var/db/config/juniper.conf.pre-install
Saving package file in
/var/sw/pkg/junos-install-x86-32-domestic-20150618.043753_builder_junos_151_r1.tgz
...
Saving state for rollback ...
```

The new Junos OS image is installed on the router.

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 newly installed version 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 package-name` command where `package` is, for example, `junos-install-mx-x86-32-15.1R1.9.tgz`. This is your last chance to stop the installation (not applicable on EX2300 and EX3400 platforms).

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.

```

user@host> show version
Hostname: host
Model: mx240
Junos: 15.1R1.9
JUNOS OS Kernel 32-bit [20150617.306001_builder_stable_10]
JUNOS OS runtime [20150617.306001_builder_stable_10]
JUNOS OS time zone information [20150617.306001_builder_stable_10]
JUNOS py base [20150618.043753_builder_junos_151_r1]
JUNOS OS crypto [20150617.306001_builder_stable_10]
JUNOS network stack and utilities [20150618.043753_builder_junos_151_r1]
JUNOS libs [20150618.043753_builder_junos_151_r1]
JUNOS runtime [20150618.043753_builder_junos_151_r1]
JUNOS platform support [20150618.043753_builder_junos_151_r1]
JUNOS modules [20150618.043753_builder_junos_151_r1]
JUNOS daemons [20150618.043753_builder_junos_151_r1]
JUNOS Voice Services Container package [20150618.043753_builder_junos_151_r1]
JUNOS Services SSL [20150618.043753_builder_junos_151_r1]
JUNOS Services Stateful Firewall [20150618.043753_builder_junos_151_r1]
JUNOS Services RPM [20150618.043753_builder_junos_151_r1]
JUNOS Services PTSP Container package [20150618.043753_builder_junos_151_r1]
JUNOS Services NAT [20150618.043753_builder_junos_151_r1]
JUNOS Services Mobile Subscriber Service Container package
[20150618.043753_builder_junos_151_r1]
JUNOS Services MobileNext Software package
[20150618.043753_builder_junos_151_r1]
JUNOS Services LL-PDF Container package
[20150618.043753_builder_junos_151_r1]
JUNOS Services Jflow Container package [20150618.043753_builder_junos_151_r1]
JUNOS Services IPSec [20150618.043753_builder_junos_151_r1]
JUNOS IDP Services [20150618.043753_builder_junos_151_r1]
JUNOS Services HTTP Content Management package
[20150618.043753_builder_junos_151_r1]
JUNOS Services Crypto [20150618.043753_builder_junos_151_r1]
JUNOS Services Captive Portal and Content Delivery Container package
[20150618.043753_builder_junos_151_r1]
JUNOS Border Gateway Function package [20150618.043753_builder_junos_151_r1]
JUNOS AppId Services [20150618.043753_builder_junos_151_r1]
JUNOS Services Application Level Gateways
[20150618.043753_builder_junos_151_r1]
JUNOS Services ACL Container package [20150618.043753_builder_junos_151_r1]
JUNOS Packet Forwarding Engine Support (MX/EX92XX Common)
[20150618.043753_builder_junos_151_r1]
JUNOS Packet Forwarding Engine Support (M/T Common)
[20150618.043753_builder_junos_151_r1]
JUNOS Online Documentation [20150618.043753_builder_junos_151_r1]
JUNOS FIPS mode utilities [20150618.043753_builder_junos_151_r1]

```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of an Earlier Release



NOTE: If you have important files in other directories, copy them from the router or switch to a secure location before upgrading the router or switch.



NOTE: The following procedure refers to routers, but it also applies to switches.

To install Junos OS with upgraded FreeBSD over Junos OS with upgraded FreeBSD of an earlier release:

1. Enter the **request system software add *package-name* validate reboot** command from the operational mode in the CLI:



NOTE: The **no-copy** option is enabled by default.

Use the **validate** and **reboot** options with the **request system software add** command. The command uses the **validate** option by default. We encourage users to validate using the **validate** option when upgrading from Junos OS to Junos OS or from Junos OS with upgraded FreeBSD to Junos OS with upgraded FreeBSD.

If you leave out the **reboot** option, you can take care of that in a separate reboot step.

The new Junos OS image is installed on the router.

2. Verify the installation of Junos OS with upgraded FreeBSD.

```
user@host> show version
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of a Later Release



NOTE: If you have important files in other directories, copy them from the router or switch to a secure location before upgrading the router or switch.



NOTE: The following procedure refers to routers, but it also applies to switches.

To install Junos OS with upgraded FreeBSD over Junos OS with upgraded FreeBSD of a later release:

1. Enter the **request system software add *package-name* validate reboot** command from the operational mode in the CLI:



NOTE: The **no-copy** option is enabled by default.

Use the **validate** and **reboot** options with the **request system software add** command. The command uses the **validate** option by default. We encourage users to validate using the **validate** option when upgrading from Junos OS to Junos OS or from Junos OS with upgraded FreeBSD to Junos OS with upgraded FreeBSD.

If you leave out the **reboot** option, you can take care of that in a separate reboot step.

The new Junos OS image is installed on the router.

2. Verify the installation of Junos OS with upgraded FreeBSD.

```
user@host> show version
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

Related Documentation

- [Downgrading Junos OS from Upgraded FreeBSD on page 209](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 327](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 314](#)

Understanding Junos OS Upgrades for SRX Series Devices

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

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.

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.



NOTE: Junos OS Release 12.1X45 and later do not support single root partitioning.

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 is preserved. Any important data must 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 for SRX Series Devices on page 10](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 153](#)

Preparing Your SRX Series Device for Junos OS Upgrades

Before you begin upgrading Junos OS on 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.

Secondary Storage Devices Available on SRX Series Devices

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 22 on page 148 lists the secondary storage devices available on an SRX Series devices.

Table 22: Secondary Storage Devices for SRX Series Devices

Storage Device	Available on Services Gateways	Minimum Storage Required
USB storage device	SRX300, SRX320, SRX340, and SRX345 Services Gateways	1 GB
	SRX550M	2 GB
SSD Card	SRX1500	100 GB
	SRX4100, SRX4200	240 GB
Routing Engine (RE2) SSD card	SRX5000 line devices	120 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.

Verifying Available Disk Space on SRX Series Devices

The amount of free disk space necessary to upgrade a device with a new version of 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 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-b1ocks      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/
prodfs	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

Cleaning Up the System File Storage Space

When the system file storage space on the device is full, rebooting the device does not solve the problem. The following error message is displayed during a typical operation on the device after the file storage space is full.

```
user@host% cli
user@host> configure/var: write failed, filesystem is full
```

You can clean up the file storage on the device by deleting system files using the **request system storage cleanup** command as shown in following procedure:

1. Request to delete system files on the device.

```
user@host> request system storage cleanup
```

The list of files to be deleted is displayed.

List of files to delete:

Size	Date	Name
11B	Oct 28 23:40	/var/jail/tmp/alarmd.ts
92.4K	Jan 11 17:12	/var/log/chassisd.0.gz
92.4K	Jan 11 06:06	/var/log/chassisd.1.gz
92.5K	Jan 10 19:00	/var/log/chassisd.2.gz
92.5K	Jan 10 07:53	/var/log/chassisd.3.gz
92.2K	Jan 10 15:00	/var/log/hostlogs/auth.log.1.gz
92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.2.gz
92.1K	Jan 4 17:30	/var/log/hostlogs/auth.log.3.gz
92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.4.gz
79.0K	Jan 12 01:59	/var/log/hostlogs/daemon.log.1.gz
78.8K	Jan 11 23:15	/var/log/hostlogs/daemon.log.2.gz
78.7K	Jan 11 20:30	/var/log/hostlogs/daemon.log.3.gz
79.1K	Jan 11 17:44	/var/log/hostlogs/daemon.log.4.gz
59.1K	Jan 11 21:59	/var/log/hostlogs/debug.1.gz
59.2K	Jan 11 17:44	/var/log/hostlogs/debug.2.gz
59.2K	Jan 11 13:29	/var/log/hostlogs/debug.3.gz
59.3K	Jan 11 09:14	/var/log/hostlogs/debug.4.gz
186.6K	Oct 20 16:31	/var/log/hostlogs/kern.log.1.gz
238.3K	Jan 11 23:15	/var/log/hostlogs/lcmd.log.1.gz
238.4K	Jan 11 17:30	/var/log/hostlogs/lcmd.log.2.gz
238.6K	Jan 11 11:45	/var/log/hostlogs/lcmd.log.3.gz
238.5K	Jan 11 06:00	/var/log/hostlogs/lcmd.log.4.gz
372.5K	Jan 11 17:00	/var/log/hostlogs/syslog.1.gz
372.5K	Jan 11 04:45	/var/log/hostlogs/syslog.2.gz

```
371.9K Jan 10 16:30 /var/log/hostlogs/syslog.3.gz
372.7K Jan 10 04:15 /var/log/hostlogs/syslog.4.gz
10.1K Jan 12 02:03 /var/log/messages.0.gz
55.1K Jan 6 21:25 /var/log/messages.1.gz
81.5K Dec 1 21:30 /var/log/messages.2.gz
```

Delete these files ? [yes,no] (no)

2. Enter the option **yes** to proceed with deleting of the files.

Downloading Software Packages from Juniper Networks

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 SRX Series Devices on page 145](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 153](#)

Example: Installing Junos OS Upgrade Packages on SRX Series Devices

This example shows how to install Junos OS upgrades on SRX Series devices.

- [Requirements on page 150](#)
- [Overview on page 151](#)
- [Configuration on page 151](#)
- [Verification on page 152](#)

Requirements

Before you begin:

- Verify the available space on the internal media. See "[Preparing Your SRX Series Device for Junos OS Upgrades](#)" on page 147 and the *Junos OS Release Notes*

- Download the software package. See “[Downloading Software Packages from Juniper Networks](#)” on page 150.
- 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) with the following options:

- **no-copy** option to install the software package but do not save the copies of package files. You must 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 configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

From operational mode, enter:

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

GUI Step-by-Step Procedure

To install Junos OS upgrades on 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*.

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
```

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 152](#)

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 SRX Series Devices on page 145](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 66](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Configure Administration User Accounts on page 174](#)

Installing Junos OS Upgrade Packages on SRX Series 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. See “[Preparing Your SRX Series Device for Junos OS Upgrades](#)” on page 147 and the *Junos OS Release Notes*
- Download the software package. See “[Downloading Software Packages from Juniper Networks](#)” on page 150.

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 23 on page 153](#).

Table 23: 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: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i>
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.

Table 23: Install Package Summary (continued)

Field	Function	Your Action
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 SRX Series Devices on page 150](#)
- [Configure Administration User Accounts on page 174](#)

Understanding BIOS Upgrades on SRX Series Devices

Understanding Manual BIOS Upgrade Using the Junos CLI

For these SRX Series devices, the BIOS consists of a U-boot and the Junos loader. The SRX300, and SRX320 Service Gateways also include a U-shell binary as part of the BIOS. Additionally, on SRX300, SRX320, SRX340, and SRX345 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 24 on page 154 Lists the CLI commands used for manual BIOS upgrade.

Table 24: CLI Commands for Manual BIOS Upgrade

Active BIOS	Backup BIOS
<code>request system firmware upgrade re bios</code>	<code>request system firmware upgrade re bios backup</code>

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.



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.
3. Upgrade the BIOS (Active and backup) image.

Active BIOS:

1. Initiate the upgrade using the **request system firmware upgrade re bios** command.
2. Monitor the upgrade status using the **show system firmware** command.



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 upgrade re bios backup** command.
2. Monitor the upgrade status using the **show system firmware** command.

Understanding Auto BIOS Upgrade Methods on SRX Series Devices

The BIOS version listed in the **bios-autoupgrade.conf** file is the minimum supported version. 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 the latest version.

The BIOS upgrades automatically in the following scenarios:

- During Junos OS upgrade through either the J-Web user interface or the CLI (using the **request system software add no-copy no-validate software-image**). In this case, only the active BIOS is upgraded.
- During loader installation using TFTP or USB (using the **install tftp:///software-image** command). In this case, only the active BIOS is upgraded.
- During system boot-up. In this case, both the active BIOS and the backup BIOS are upgraded.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Installing Junos OS on SRX Series Devices Using a USB Flash Drive on page 68](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 70](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 72](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 156](#)

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, use the **chassis routing-engine bios** command as following:

```
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.

To disable the user inputs at u-boot and bootloader stage, use the **chassis routing-engine bios** command as following:

```
user@host> set chassis routing-engine bios uninterrupt
```

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Understanding BIOS Upgrades on SRX Series Devices on page 154](#)

Example: Downgrading Junos OS on SRX Series Devices

This example shows how to downgrade Junos OS on the SRX Series devices.

- [Requirements on page 156](#)
- [Overview on page 156](#)
- [Configuration on page 157](#)
- [Verification on page 158](#)

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

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*.

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 158](#)

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**
- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)
 - [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
 - [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
 - [Restarting and Halting SRX Series Devices on page 213](#)

Booting a Device Using a System Snapshot

- [Understanding System Snapshot on EX Series Switches on page 159](#)
- [Creating a Snapshot and Using It to Boot an EX Series Switch on page 160](#)
- [Verifying That a System Snapshot Was Created on an EX Series Switch on page 161](#)
- [Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive on page 162](#)

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**, and **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 Chassis 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 44](#)
- [Creating a Snapshot and Using It to Boot an EX Series Switch on page 160](#)

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 160](#)

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 usb
```
2. (Optional) Perform this step if you want to boot the switch now using the snapshot stored on the USB flash drive.

```
user@switch> request system reboot media usb
```

Related Documentation

- [Verifying That a System Snapshot Was Created on an EX Series Switch on page 161](#)
- [Understanding System Snapshot on EX Series Switches on page 159](#)

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 160](#)

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 160](#). 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 51](#).
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 \(CLI Procedure\)](#)
- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)

- 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.

Performing a Recovery Installation

- [Creating an Emergency Boot Device on page 165](#)
- [Configuring Boot Devices for SRX Series Devices on page 166](#)
- [Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices on page 169](#)
- [Performing a Recovery Installation on page 172](#)
- [Creating a New Configuration on a Single Routing Engine on page 173](#)
- [Creating a New Configuration with Redundant Routing Engines on page 178](#)
- [Saving a Rescue Configuration File on page 183](#)
- [Restoring a Saved Configuration on page 184](#)
- [Reverting to the Default Factory Configuration by Using the request system zeroize Command on page 185](#)
- [Reverting to the Rescue Configuration on page 186](#)

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 32.
- **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
```

Configuring Boot Devices for SRX Series Devices

This topic includes the following sections:

- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)

Example: Creating a Snapshot and Using It to Boot an SRX Series Device

This example shows how to configure a boot device.

- [Requirements on page 166](#)
- [Overview on page 167](#)
- [Configuration on page 167](#)
- [Creating a Snapshot on a USB Flash Drive and Using It to Boot the SRX Series Device on page 168](#)
- [Verification on page 169](#)

Requirements

Before you begin, ensure that the backup device has a storage capacity of at least 1 GB. See “Preparing Your SRX Series Device for Junos OS Upgrades” on page 147.

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

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*.

To configure a boot device:

```
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.

[Creating a Snapshot on a USB Flash Drive and Using It to Boot the SRX Series Device](#)

Step-by-Step Procedure You can create a snapshot on a USB flash drive and use it to boot the SRX series device.

To create a snapshot on a USB flash memory and use it to boot the SRX series device:

1. Place the snapshot into USB flash memory:

```
user@host> request system snapshot partition media USB
```
2. (Optional) Perform this step, if you want to boot the SRX now using the newly created snapshot on the USB flash drive. If you created the snapshot as a backup, do not perform this step.
 - To reboot the SRX using the most recently created snapshot:

```
user@host> request system reboot media USB
```

Verification

Confirm that the configuration is working properly.

- [Verifying the Snapshot Information on page 169](#)

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.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)

Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices

This topic includes the following sections:

- [Overview on page 170](#)
- [How Autorecovery Works on page 170](#)

- [How to Use Autorecovery on page 170](#)
- [Data That Is Backed Up in an Autorecovery on page 171](#)
- [Troubleshooting Alarms on page 171](#)
- [Considerations on page 171](#)

Overview

The autorecovery feature is supported on dual-partitioned SRX Series devices. 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 labels (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 25 on page 171 lists types of autorecovery alarms, descriptions, and required actions.

Table 25: Autorecovery Alarms

Alarm	Alarm Type	Description	Action Required
Autorecovery information needs to be saved	Minor	This alarm indicates: <ul style="list-style-type: none"> • Unsaved data needs to be saved, or saved data contains problems and another save is required. 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Boot time integrity check failed for certain items; however, the items have been recovered successfully. 	<ul style="list-style-type: none"> • No action is required. • Alarm is cleared on next bootup.
Autorecovery was unable to recover data completely	Major	This alarm indicates: <ul style="list-style-type: none"> • Boot time integrity check failed for certain items, which could not be recovered successfully. 	<ul style="list-style-type: none"> • 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 must 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

- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 156](#)

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 165](#)
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 device 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 173](#), [“Creating a New Configuration with Redundant Routing Engines” on page 178](#), and [“Restoring a Saved Configuration” on page 184](#).

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 173](#)
- [Configure Administration User Accounts on page 174](#)
- [Add the Management Console to the Network on page 174](#)
- [Commit Changes on page 176](#)

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.device1.example.com;
  backup-router 192.168.71.254;
  root-authentication {
    encrypted-password "$ABC123"; ## SECRET-DATA
  }
  name-server {
    192.168.5.68;
    172.17.28.101;
  }
  login {
    user PE1 {
      class super-user;
      authentication {
        encrypted-password "$ABC123"; ## 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 178](#)
- [Set Up Routing Engine Configuration Groups on page 179](#)
- [Complete the Management Console Configuration on page 180](#)
- [Commit and Synchronize Changes on page 181](#)

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
```

- Return to the top level of the hierarchy.

```
[edit groups re0]
root# top
```

- Create the configuration group **re1**.

```
[edit]
root# set groups re1
```

- Navigate to the **groups re1** level of the configuration hierarchy.

```
[edit]
root# edit groups re1
```

- Specify the router hostname.

```
[edit groups re1]
root# set system host-name host-name
```

- 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
```

- Return to the top level of the hierarchy.

```
[edit groups re0]
root# top
```

- Specify the group application order.

```
[edit]
root# set apply-groups [ re0 re1 ]
```

Complete the Management Console Configuration

To configure the global management console parameters.

- Configure the IP address of the DNS server.

```
[edit]
root# set system name-server address
```

- 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 "$ABC123"; ## SECRET-DATA
    }
    name-server {
        192.168.1.1;
    }
    login {
        user user1 {
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "$ABC123"; ## 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 184](#)
2. [Loading and Committing the Configuration File on page 185](#)

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.
```

Loading and Committing 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 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 375](#)

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

- [Reverting to the Default Factory Configuration](#)

CHAPTER 11

Reinstalling Software

- Checklist for Reinstalling Junos OS on page 187
- Log the Software Version Information on page 189
- Log the Hardware Version Information on page 190
- Log the Chassis Environment Information on page 191
- Log the System Boot-Message Information on page 192
- Log the Active Configuration on page 194
- Log the Interfaces on the Router on page 194
- Log the BGP, IS-IS, and OSPF Adjacency Information on page 195
- Log the System Storage Information on page 196
- Back Up the Currently Running and Active File System on page 197
- Reinstall Junos OS on page 197
- Reconfigure Junos OS on page 198
- Configure Host Names, Domain Names, and IP Addresses on page 202
- Protecting Network Security by Configuring the Root Password on page 204
- Check Network Connectivity on page 206
- Copy Backup Configurations to the Router on page 206
- After You Reinstall Junos OS on page 206
- Compare Information Logged Before and After the Reinstall on page 207
- Back Up the New Software on page 207

Checklist for Reinstalling Junos OS

Table 26 on page 187 provides links and commands for reinstalling Junos OS.

Table 26: Checklist for Reinstalling Junos OS

Tasks	Command or Action
Before You Reinstall Junos OS	
1. Log the Software Version Information on page 189	<code>show version</code> <code>save filename</code>

Table 26: Checklist for Reinstalling Junos OS (*continued*)

Tasks	Command or Action
2. Log the Hardware Version Information on page 190	<code>show chassis hardware save filename</code>
3. Log the Chassis Environment Information on page 191	<code>show chassis environment save filename</code>
4. Log the System Boot-Message Information on page 192	<code>show system boot-messages save filename</code>
5. Log the Active Configuration on page 194	<code>show configuration save filename</code>
6. Log the Interfaces on the Router on page 194	<code>show interface terse save filename</code>
7. Log the BGP, IS-IS, and OSPF Adjacency Information on page 195	<code>show bgp summary save filename</code> <code>show isis adjacency brief save filename</code> <code>show ospf neighbor brief save filename</code>
8. Log the System Storage Information on page 196	<code>show system storage save filename</code>
9. Back Up the Currently Running and Active File System on page 197	<code>request system snapshot</code>
10.	http://www.juniper.net/support
“Reinstall Junos OS” on page 197	Insert the floppy and reboot the system.
“Reconfigure Junos OS” on page 198	
1. Configure Host Names, Domain Names, and IP Addresses on page 198	Log in as root. Start the CLI. Enter configuration mode: <code>configure</code> <code>set system host-name host-name</code> <code>set system domain-name domain-name</code> <code>set interfaces fxp0 unit 0 family inet address address/prefix-length</code> <code>set system backup-router address</code> <code>set system name-server address</code>
2. Protecting Network Security by Configuring the Root Password on page 200	<code>set system root-authentication plain-text-password</code> <code>set system root-authentication encrypted-password password</code> <code>set system root-authentication ssh-rsa key</code> <code>commit</code> <code>exit</code>
3. Check Network Connectivity on page 201	<code>ping address</code>
4. Copy Backup Configurations to the Router on page 202	<code>file copy var/tmp</code> <code>configure</code> [edit] <code>load merge /config/filename</code> or <code>load replace /config/filename</code> [edit] <code>commit</code>

Table 26: Checklist for Reinstalling Junos OS (*continued*)

Tasks	Command or Action
“After You Reinstall Junos OS” on page 206	
1. Compare Information Logged Before and After the Reinstall on page 206	<pre>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</pre>
2. Back Up the New Software on page 207	<pre>request system snapshot</pre>

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
BPDELAYD 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              REV 02   710-001245   101            M160
Midplane             REV 01   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                REV 02   710-001611   S/N AA9523      FPC Type 2
CPU                  REV 03   710-001217   S/N AB3329
PIC 0                REV 01   710-001217   S/N AB3329      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@device1.example.com: /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,VE,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 ctrlr(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 device1.example.com;
  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       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
procfss      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 198](#)
2. [Protecting Network Security by Configuring the Root Password on page 200](#)
3. [Check Network Connectivity on page 201](#)
4. [Copy Backup Configurations to the Router on page 202](#)

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
```

Protecting Network Security by Configuring the Root Password

Configuring the root password on your Junos OS-enabled router helps prevent unauthorized users from making changes to your network. The root user (also referred to as superuser) has unrestricted access and full permissions within the system, so it is crucial to protect these functions by setting a strong password when setting up a new router.

After a new router is initially powered on, you log in as the user **root** with no password. 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 a few options as shown in Step 1 of the following procedure.

- Enter a plain-text password that Junos OS encrypts.
- Enter a password that is already encrypted.
- Enter a secure shell (ssh) public key string.

The most secure options of these three are using an already encrypted password or an ssh public key string. Pre-encrypting your password or using a ssh public key string means the plain-text version of your password will never be transferred over the internet, protecting it from being intercepted by a man-in-the-middle attack.



BEST PRACTICE: Optionally, instead of configuring the root password at the `[edit system]` hierarchy level, you can use a configuration group to strengthen security, as shown in Step 2 of this procedure. This step uses a group called **global** as an example.

To set the root password:

1. Use one of these methods to configure the root password:

- To enter a plain-text password that the system encrypts for you:

```
[edit groups global system]
root@# set root-authentication plain-text-password
New Password: type password here
Retype new password: retry password here
```

If you use a plain-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:



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 plain-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 key string:

```
[edit groups global system]
root@# set root-authentication (ssh-dsa | ssh-eccdsa | 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 in Step 2, 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
```

Protecting Network Security by Configuring the Root Password

Configuring the root password on your Junos OS-enabled router helps prevent unauthorized users from making changes to your network. The root user (also referred to as superuser) has unrestricted access and full permissions within the system, so it is crucial to protect these functions by setting a strong password when setting up a new router.

After a new router is initially powered on, you log in as the user **root** with no password. 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 a few options as shown in Step 1 of the following procedure.

- Enter a plain-text password that Junos OS encrypts.
- Enter a password that is already encrypted.
- Enter a secure shell (ssh) public key string.

The most secure options of these three are using an already encrypted password or an ssh public key string. Pre-encrypting your password or using a ssh public key string means the plain-text version of your password will never be transferred over the internet, protecting it from being intercepted by a man-in-the-middle attack.



BEST PRACTICE: Optionally, instead of configuring the root password at the `[edit system]` hierarchy level, you can use a configuration group to strengthen security, as shown in Step 2 of this procedure. This step uses a group called `global` as an example.

To set the root password:

1. Use one of these methods to configure the root password:

- To enter a plain-text password that the system encrypts for you:

```
[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 plain-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:



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 plain-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 key string:

```
[edit groups global system]
root@# set root-authentication (ssh-dsa | ssh-eccdsa | 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 in Step 2, 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 206](#)
2. [Back Up the New Software on page 207](#)

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.

Downgrading Software

- [Downgrading Junos OS from Upgraded FreeBSD on page 209](#)

Downgrading Junos OS from Upgraded FreeBSD

Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. If you have previously upgraded to Junos OS with upgraded FreeBSD, you can downgrade to earlier versions of Junos OS, as long as the downgrade conforms to the Junos OS policy of skipping at most two earlier releases.

Before you begin:

1. Verify that you have previously upgraded to Junos OS with the upgraded FreeBSD kernel, as described in [“Upgrading Junos OS with Upgraded FreeBSD” on page 139](#).
2. Download the Junos OS package.

Select and perform the procedure that matches your conditions:

- [Downgrading from Junos OS with Upgraded FreeBSD to Junos OS on page 209](#)
- [Downgrading from Junos OS with Upgraded FreeBSD to an Earlier Release of Junos OS with Upgraded FreeBSD on page 211](#)

Downgrading from Junos OS with Upgraded FreeBSD to Junos OS

This example uses the package `/var/tmp/jinstall-13.3R2.7-domestic-signed.tgz` to install Junos OS with a pre-upgraded FreeBSD kernel on the master Routing Engine (re0).



NOTE: The following procedure refers to routers, but it also applies to switches.

To downgrade from Junos OS with upgraded FreeBSD to Junos OS:

1. Enter the `request system software add package-name no-validate reboot` command from the operational mode in the CLI.

Use the `no-validate` and `reboot` options with the `request system software add` command. If you leave out the `no-validate` option, the command uses the `validate` option by

default, and direct validation of running configuration does not work for downgrading to Junos OS from Junos OS with upgraded FreeBSD.



NOTE: To validate current configuration on an downgrade to Junos OS from Junos OS with upgraded FreeBSD, use the `request system software validate on (Junos OS with Upgraded FreeBSD)` command.

If you leave out the `reboot` option, you can take care of that in a separate reboot step.

The following example uses the `re0` option:

```
user@host>request system software add
/var/tmp/jinstall-13.3R2.7-domestic-signed.tgz re0 no-validate reboot
THIS IS A SIGNED PACKAGE Saving the config files ...
NOTICE: uncommitted changes have been saved in
/var/db/config/juniper.conf.pre-install Rebooting. Please wait ...
shutdown: [pid 11001] Shutdown NOW! *** FINAL System shutdown message
from root@host *** System going down IMMEDIATELY Shutdown NOW! System
shutdown time has arrived\x07\x07 users@host> Connection to
device1.example.com closed by remote host. Connection to
device1.example.com closed. ... user@router> show version
Hostname: host
Model: mx240
Junos: 13.3R2.7
JUNOS Base OS boot [13.3R2.7]
JUNOS Base OS Software Suite [13.3R2.7]
JUNOS Kernel Software Suite [13.3R2.7]
JUNOS Crypto Software Suite [13.3R2.7]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [13.3R2.7]
JUNOS Packet Forwarding Engine Support (MX Common) [13.3R2.7]
JUNOS Online Documentation [13.3R2.7]
JUNOS Services AACL Container package [13.3R2.7]
...
```

2. Verify the downgrade of the software package.

```
user@host> show version
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

Downgrading from Junos OS with Upgraded FreeBSD to an Earlier Release of Junos OS with Upgraded FreeBSD

This example uses the package `/var/tmp/jinstall-13.3R2.7-domestic-signed.tgz` to install Junos OS with a pre-upgraded FreeBSD kernel on the master Routing Engine (re0).



NOTE: The following procedure refers to routers, but it also applies to switches.

To downgrade from Junos OS with upgraded FreeBSD to an earlier release of Junos OS with upgraded FreeBSD:

1. Enter the `request system software add package-name validate reboot` command from the operational mode in the CLI:

Use the `validate` and `reboot` options with the `request system software add` command. The command uses the `validate` option by default.

If you leave out the `reboot` option, you can take care of that in a separate reboot step.

2. Verify the downgrade of the software package.

```
user@host> show version
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

Related Documentation

- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 327](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 314](#)

Rebooting or Halting Software Processes on a Device

- [Restarting and Halting SRX Series Devices on page 213](#)
- [Rebooting or Halting the EX Series Switch \(J-Web Procedure\) on page 218](#)

Restarting and Halting SRX Series Devices

This topic includes the following sections:

- [Rebooting SRX Series Devices on page 213](#)
- [Halting SRX Series Devices on page 215](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 217](#)
- [Restarting the Chassis on SRX Series Devices on page 217](#)

Rebooting SRX Series Devices

This example shows how to reboot a SRX Series device.

- [Requirements on page 213](#)
- [Overview on page 213](#)
- [Configuration on page 213](#)
- [Verification on page 215](#)

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

CLI Quick Configuration To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your

network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

From operational mode, enter:

```
user@host> request system reboot at 5 in 50 media internal 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) 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.

Enter:

```
user@host> request system reboot at 5 in 50 media internal 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 215](#)

Verifying the Device Reboot

Purpose Verify that the device rebooted.

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

Halting SRX Series Devices

This example shows how to halt a device.

- [Requirements on page 215](#)
- [Overview on page 215](#)
- [Configuration on page 215](#)
- [Verification on page 216](#)

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

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

From operational mode, enter:

```
user@host>request system halt at now
```



NOTE: The `request system halt` command used for halting the system and stopping software processes on the device is not supported on SRX1500, SRX4100, and SRx4200 devices.

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 216](#)

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 SRX Series Devices

You can use the **request** commands to bring chassis components online and offline.

To bring chassis components online and offline, enter these **request chassis** commands:

```
user@host> request chassis <fru> slot <slot#> pic <pic#> online
```

```
user@host> request chassis <fru> slot <slot#> pic <pic#> offline
```

Where **<fru>** in the request chassis command can be any of the following (for Branch SRX Series devices):

- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.

Where **<fru>** in the request chassis command can be any of the following (for High-End SRX Series devices):

- **cb**—Changes the control board 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.



NOTE: The **request chassis** command is not supported for bringing SPCs online and offline.

Example:

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 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

- [Software License Overview on page 221](#)
- [Installing and Managing Licenses on page 255](#)

Software License Overview

- [Junos OS Feature Licenses on page 221](#)
- [License Enforcement on page 222](#)
- [Junos OS Feature License Keys on page 223](#)
- [Software Feature Licenses on page 226](#)
- [Understanding Software Licenses for EX Series Switches on page 244](#)

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 222](#)
- [Junos OS Feature License Model Number for SRX Series Services Gateways on page 234](#)
- [Adding New Licenses \(CLI Procedure\) on page 255](#)
- [Deleting a License \(CLI Procedure\) on page 256](#)
- [Saving License Keys on page 257](#)
- [Verifying Junos OS License Installation on page 258](#)

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 device 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 221](#)
- [Software Feature Licenses on page 226](#)
- [Adding New Licenses \(CLI Procedure\) on page 255](#)
- [Deleting a License \(CLI Procedure\) on page 256](#)
- [Saving License Keys on page 257](#)
- [Verifying Junos OS License Installation on page 258](#)

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 27 on page 225](#) 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 27: 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 <ul style="list-style-type: none"> 1/MIC0 	f1—MX5 to MX10 upgrade	Slot 1 and 2 <ul style="list-style-type: none"> 1/MIC0 1/MIC1
MX10	40G	0x555	Slot 1 and 2 <ul style="list-style-type: none"> 1/MIC0 1/MIC1 	f2—MX10 to MX40 upgrade	Slot 2 and first 2 ports on Slot 0 <ul style="list-style-type: none"> 1/MIC1 First 2 ports on 0/MIC0
MX40	60G	0x554	Slot 1, Slot 2 and first 2 ports on Slot 0 <ul style="list-style-type: none"> 1/MIC0 1/MIC1 First 2 ports on 0/MIC0 	f3—MX40 to MX80 upgrade	Slot 2 and all ports on Slot 0 <ul style="list-style-type: none"> 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 28 on page 226](#).

Table 28: 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 28 on page 226](#) 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 221](#)
- [License Enforcement on page 222](#)
- [Software Feature Licenses on page 226](#)
- [Verifying Junos OS License Installation on page 258](#)
- [show system license on page 396](#)

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 226](#)
- [Software Features That Require Licenses on M Series Routers Only on page 229](#)
- [Software Features That Require Licenses on MX Series Routers Only on page 230](#)
- [Software Feature Licenses for SRX Series Devices on page 234](#)
- [Software Features That Require Licenses on EX Series Switches on page 239](#)
- [Software Features That Require Licenses on the QFX Series on page 241](#)

Software Features That Require Licenses on M Series, MX Series, and T Series Routers

[Table 29 on page 227](#) 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 29: 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 functionality, 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 functionality, 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 29: 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 Upgrade 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 Upgrade 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 29: 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 30 on page 230 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 30: 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 31 on page 231 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 31: 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 31: 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 31: 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 31: 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 Feature Licenses for 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 32 on page 234 describes the Junos OS features that require licenses.

Table 32: Junos OS Feature Licenses

Junos OS License Requirements			
Feature	SRX550M	SRX1500	SRX5000 line
Access Manager	X		
BGP Route Reflectors			
Dynamic VPN	X		
IDP Signature Update*	X	X	X

Table 32: Junos OS Feature Licenses (*continued*)

Junos OS License Requirements			
Feature	SRX550M	SRX1500	SRX5000 line
Application Signature Update (Application Identification)*	X		X
Juniper-Kaspersky Antivirus*	X		
Juniper-Sophos Antivirus*	X	X	X
Juniper-Sophos Antispam*	X	X	X
Juniper-Enhanced Web filtering*	X	X	X
Juniper-Websense Web filtering*	X		
Logical Systems			X
UTM	X	X	X

* Indicates support on high-memory devices only.

Table 33 on page 236 lists the licenses you can purchase for each SRX Series software feature. Each license allows you to run the specified advanced software features 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 33: Junos OS Feature License Model Number for SRX Series Devices

Licensed Software Feature	Supported Devices	Model Number
Application Security and IDP updates (1 year, 3 years, and 5 years)	SRX550	SRX550-APPSEC-A-1
		SRX550-APPSEC-A-3
		SRX550-APPSEC-A-5
	SRX5400	SRX5400-APPSEC-1
		SRX5400-APPSEC-3
		SRX5400-APPSEC-5
	SRX5600	SRX5600-APPSEC-A-1
		SRX5600-APPSEC-A-3
		SRX5600-APPSEC-A-5
	SRX5800	SRX5800-APPSEC-A-1
		SRX5800-APPSEC-A-3
		SRX5800-APPSEC-A-5
IDP updates (1 year, 3 years, and 5 years)	SRX550	SRX550-IDP
		SRX550-IDP-3
		SRX550-IDP-5
IDP subscription (1 year and 3 years)	SRX1500	SRX1500-IPS-1
		SRX1500-IPS-3
	SRX5400, SRX5600, SRX5800	SRX5K-IDP
		SRX5K-IDP-3
		SRX5K-IDP-3-R
		SRX5K-IDP-R
Juniper-Kaspersky Antivirus updates (1 year, 3 years, and 5 years)	SRX550	SRX550-K-AV
		SRX550-K-AV-3
		SRX550-K-AV-5
Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years)	SRX550	SRX550-S-AV
		SRX550-S-AV-3
		SRX550-S-AV-5

Table 33: Junos OS Feature License Model Number for SRX Series Devices (continued)

Licensed Software Feature	Supported Devices	Model Number
Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years)	SRX5400	SRX5400-S-AV-1
		SRX5400-S-AV-3
		SRX5400-S-AV-5
Juniper-Sophos Antivirus updates (1 year)	SRX5600	SRX5600-S-AV-1
	SRX5800	SRX5800-S-AV-1
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX550	SRX550-S2-AS
		SRX550-S2-AS-3
		SRX550-S2-AS-5
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX5400	SRX5400-S-AV-1
		SRX5400-S-AV-3
		SRX5400-S-AV-5
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX5600	SRX5600-S-AV-1
	SRX5800	SRX5800-S-AV-1
Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years)	SRX550	SRX550-W-EWF
		SRX550-W-EWF-3
		SRX550-W-EWF-5
Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years)	SRX5400	SRX5400-W-EWF-1
		SRX5400-W-EWF-3
		SRX5400-W-EWF-5
Juniper-Enhanced Web filtering (1 year)	SRX5600	SRX5600-W-EWF-1
	SRX5800	SRX5800-W-EWF-1
Enterprise Bundle—Kaspersky Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX550	SRX550-SMB4-CS
		SRX550-SMB4-CS-3
		SRX550-SMB4-CS-5

Table 33: Junos OS Feature License Model Number for SRX Series Devices (continued)

Licensed Software Feature	Supported Devices	Model Number
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX550	SRX550-S-SMB4- CS
		SRX550-S-SMB4- CS-3
		SRX550-S-SMB4- CS-5
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years)	SRX1500	SRX1500-CS-BUN-1
		SRX1500-CS-BUN-3
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX5400	SRX5400-CS-BUN-1
		SRX5400-CS-BUN-3
		SRX5400-CS-BUN-5
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year)	SRX5600	SRX5600-CS-BUN-1
	SRX5800	SRX5800-CS-BUN-1
Dynamic VPN Client (5, 10, and 25 simultaneous users)	SRX550	SRX-RAC-5-LTU
		SRX-RAC-10-LTU
		SRX-RAC-25-LTU
Dynamic VPN Service (5, 10, 25, and 50 simultaneous users)	SRX550	SRX-RAC-5-LTU
	SRX550	SRX-RAC-10-LTU
	SRX550	SRX-RAC-25-LTU
	SRX550	SRX-RAC-50-LTU
Dynamic VPN Service (100 and 150 simultaneous users)	SRX550	SRX-RAC-100-LTU
		SRX-RAC-150-LTU
Dynamic VPN Service (250 simultaneous users)	SRX550	SRX-RAC-250-LTU
	NOTE: Requires Junos OS 11.2R3 or later	
Dynamic VPN Service (500 simultaneous users)	SRX550	SRX-RAC-500-LTU
	NOTE: Requires Junos OS 11.2R3 or later	

Table 33: Junos OS Feature License Model Number for SRX Series Devices (continued)

Licensed Software Feature	Supported Devices	Model Number
Express Path License (formerly known as <i>services offloading</i>)	SRX5400, SRX5600, SRX5800	SRX5K-SVCS-OFFLOAD-RTU
<p>NOTE: Prior to Junos OS Release 12.3X48-D10, Express Path was a licensed software feature. Starting with Junos OS Release 12.3X48-D10, the Express Path license is no longer required to enable this functionality. Your previously acquired Express Path license will not be effective anymore.</p>		
Logical Systems License (incremental 1, 5, and 25 numbers)	SRX5400	SRX-5400-LSYS-1
		SRX-5400-LSYS-5
		SRX-5400-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
Sky Advanced Threat protection (1 year, 3 years)	SRX1500	SRX1500-ATP-1
		SRX1500-ATP-3
Command and Control feeds (1 year, 3 years)	SRX1500	SPOT-CC-1500-1Y
		SPOT-CC-1500-3Y

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 802.1ad)
- (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 34 on page 240 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](#)” on page 244.

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 34: 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

Table 34: 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
Enhanced Feature License for EX 2200-48T/P	EX2200	EX-48-EFL
Enhanced Feature License for EX2200-C	EX2200-C	EX-12-EFL
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: Virtual Extensible Local Area Network (VXLAN) is not supported on QFX3500 and QFX3600 devices. When you issue the `show licenses` command, you will see VXLAN in the CLI output, but the feature is not enabled.



NOTE: There is no separate license for Virtual Chassis like there is for Virtual Chassis Fabric.

Table 35 on page 242 lists the standard Junos OS features licenses and supported QFX Series devices. For information on disaggregated Junos OS feature licenses on the QFX5200-32C switch, see *Disaggregated Software Features That Require Licenses on the QFX Series*.

For information about how to purchase a software license, contact your Juniper Networks sales representative.

Table 35: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series premium feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX10002-36Q switch	One per switch	QFX10002-36Q-PFL
	QFX10002-72Q switch		QFX10002-72Q-PFL
	QFX10008 switch		QFX10008-PFL
	QFX10016 switch		QFX10016-PFL
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)	QFX10002-36Q switch	One per switch	QFX10002-36Q-AFL
	QFX10002-72Q switch		QFX10002-72Q-AFL
	QFX10008 switch		QFX10008-AFL
	QFX10016 switch		QFX10016-AFL
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)	QFX5110-48S switch	One per switch	QFX5K-C1-PFL
	QFX3500, QFX3600, QFX5100-48S, and QFX5100-48T switch		QFX-JSL-EDGE-ADV1
	QFX5100-24Q and QFX5100-96S switch		QFX5100-HDNSE-LIC
	QFX5100-24Q and QFX5100-96S switch		QFX5100-HDNSE-LIC

Table 35: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
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
QFX and EX Series feature license for enabling Media Access Control security (MACsec)	QFX switches that support MACsec. See <i>Understanding Media Access Control Security (MACsec)</i> .	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

Understanding Software Licenses for EX Series Switches

To enable and use some of the Juniper Networks operating system (Junos OS) features, you must purchase, install, and manage separate software licenses. If the switch has the appropriate software license, you can configure and use these features.

The Junos OS feature license (that is, the purchased authorization code) is universal. However, to conform to Junos OS feature licensing requirements, you must install a unique license key (a combination of the authorization code and the switch's serial number) on each switch.

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 linecard role or for the redundant Routing Engine (RE) modules or the redundant Switch Fabric and Routing Engine (SRE) modules in an EX8200 member switch.

This topic describes:

- [Purchasing a Software Feature License on page 244](#)
- [Features Requiring a License on EX2200 Switches on page 245](#)
- [Features Requiring a License on EX2300 Switches on page 246](#)
- [Features Requiring a License on EX3300 Switches on page 246](#)
- [Features Requiring a License on EX3400 Switches on page 247](#)
- [Features Requiring a License on EX4300 Switches on page 248](#)
- [Features Requiring a License on EX4600 Switches on page 250](#)
- [Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches on page 251](#)
- [License Warning Messages on page 252](#)

Purchasing a Software Feature License

The following sections list features that require separate licenses. To purchase a software license, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.



NOTE: You are required to provide the 12-digit serial number when purchasing a license for an XRE200 External Routing Engine in an EX8200 Virtual Chassis.

The serial number listed on the XRE200 External Routing Engine serial ID label is 16 digits long. Use the last 12 digits of the 16-digit serial number to purchase the license.

You can use the `show chassis hardware` command output to display the 12-digit serial number of the XRE200 External Routing Engine.

Features Requiring a License on EX2200 Switches

For EX2200 switches, the following features can be added to basic Junos OS by installing an enhanced feature license (EFL):

- Bidirectional Forwarding Detection (BFD)
- Connectivity fault management (IEEE 802.1ag)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- OSPFv1/v2 (with four active interfaces)
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Q-in-Q tunneling (IEEE 802.1ad)
- Real-time performance monitoring (RPM)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 36 on page 245 lists the EFLs that you can purchase for EX2200 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX2200 switch.

Table 36: Junos OS EFL Part Number on EX2200 Switches

Switch Model	EFL Part Number
EX2200-C-12P-2G EX2200-C-12T-2G	EX-12-EFL
EX2200-24T-4G EX2200-24P-4G EX2200-24T-DC-4G	EX-24-EFL
EX2200-48T-4G EX2200-48P-4G	EX-48-EFL

Features Requiring a License on EX2300 Switches

EX2300 switches has an enhanced feature licenses (EFLs).

To use the following features on the EX2300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols: Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv6
- Multicast Source Discovery protocol (MSDP)
- OSPF v2/v3
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng
- Virtual Router Redundancy Protocol (VRRP)

[Table 37 on page 246](#) lists the EFLs that you can purchase for EX2300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX2300 switch.

Table 37: Junos OS EFL Part Number on EX2300 Switches

Switch Model	EFL Part Number
EX2300-24T	EX-24-EFL
EX2300-24P	
EX2300-C-12P	
EX2300-C-12T	

Features Requiring a License on EX3300 Switches

Two types of licenses are available on EX3300 switches: enhanced feature licenses (EFLs) and advanced feature licenses (AFLs).

To use the following features on the EX3300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols: Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv6, virtual router support for unicast and filter-based forwarding (FBF)
- OSPFv1/v2

- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Q-in-Q tunneling (IEEE 802.1ad)
- Real-time performance monitoring (RPM)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 38 on page 247 lists the EFLs that you can purchase for EX3300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX3300 switch.

Table 38: Junos OS EFL Part Number on EX3300 Switches

Switch Model	EFL Part Number
EX3300-24T EX3300-24P EX3300-24T-DC	EX-24-EFL
EX3300-48T EX3300-48T-BF EX3300-48P	EX-48-EFL

To use the following feature on EX3300 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- IPv6 routing protocols: IPv6 BGP and IPv6 for MBGP
- Virtual routing and forwarding (VRF) BGP

Table 39 on page 247 lists the AFLs that you can purchase for EX3300 switch models. For EX3300 switches, you must purchase and install a corresponding EFL along with the AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX3300 switch.

Table 39: Junos OS AFL Part Number on EX3300 Switches

Switch Model	AFL Part Number
EX3300-24T EX3300-24P EX3300-24T-DC	EX-24-AFL
EX3300-48T EX3300-48T-BF EX3300-48P	EX-48-AFL

Features Requiring a License on EX3400 Switches

EX3400 switches has an enhanced feature licenses (EFLs) and MACSec license.

To use the following features on the EX3400 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols: : Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv6, virtual router support for unicast and filter-based forwarding (FBF)
- Multicast Source Discovery Protocol (MSDP)
- OSPF v2/v3
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng
- Unicast reverse-path forwarding (RPF)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 40 on page 248 lists the EFLs that you can purchase for EX3400 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX3400 switch.

Table 40: Junos OS EFL Part Number on EX3400 Switches

Switch Model	EFL Part Number
EX3400-24T EX3400-24P	EX-24-EFL
EX3400-48T EX3400-48P EX3400-48T-AFI	EX-48-EFL

Features Requiring a License on EX4300 Switches

Two types of licenses are available on EX4300 switches: enhanced feature licenses (EFLs) and advanced feature licenses (AFLs).

To use the following features on the EX4300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- Connectivity fault management (IEEE 802.1ag)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- Multicast Source Discovery Protocol (MSDP)
- OSPFv2/v3

- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng (RIP next generation)
- Unicast reverse-path forwarding (RPF)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 41 on page 249 lists the EFLs that you can purchase for EX4300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX4300 switch.

Table 41: Junos OS EFL Part Number on EX4300 Switches

Switch Model	EFL Part Number
EX4300-24T EX4300-24P	EX4300-24-EFL
EX4300-48P EX4300-48T EX4300-48T-AFI EX4300-48T-DC EX4300-48T-DC-AFI	EX4300-48-EFL
EX4300-32F EX4300-32F-DC	EX4300-32F-EFL

To use the following features on EX4300 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)

Table 42 on page 249 lists the AFLs that you can purchase for EX4300 switch models. For EX4300 switches, you must purchase and install a corresponding EFL along with the AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX4300 switch.

Table 42: Junos OS AFL Part Number on EX4300 Switches

Switch Model	AFL Part Number
EX4300-24T EX4300-24P	EX4300-24-AFL
EX4300-48P EX4300-48T EX4300-48T-AFI EX4300-48T-DC EX4300-48T-DC-AFI	EX4300-48-AFL

Table 42: Junos OS AFL Part Number on EX4300 Switches (continued)

Switch Model	AFL Part Number
EX4300-32F EX4300-32F-DC	EX4300-32F-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4300 switches.

Features Requiring a License on EX4600 Switches

To use the following features on EX4600 switches, you must install an advanced feature license:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)
- Multiprotocol Label Switching (MPLS)

Table 43 on page 250 lists the AFLs that you can purchase for EX4600 switch models.

Table 43: Junos OS AFL Part Number on EX4600 Switches

Switch Model	AFL Part Number
EX4600-40F	EX4600-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4600 switches.

Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches

To use the following features on EX3200, EX4200, EX4500, EX4550, EX8200, and EX9200 switches, you must install an advanced feature license (AFL):

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Ethernet VPN (available only on EX9200 switches)
- Intermediate System-to-Intermediate System (IS-IS)
- IPv6 routing protocols: IS-IS for IPv6, IPv6 BGP, IPv6 for MBGP
- Logical systems (available only on EX9200 switches)
- MPLS with RSVP-based label-switched paths (LSPs) and MPLS-based circuit cross-connects (CCCs) (Not supported on EX9200 switches)
- Open vSwitch Database (OVSDB) (available only on EX9200 switches)
- Virtual Extensible LAN (VXLAN) (available only on EX9200 switches)

To use the following features on Juniper Networks EX6200 Ethernet Switches, you must install an advanced feature license (AFL):

- Border Gateway Protocol (BGP)
- Intermediate System-to-Intermediate System (IS-IS)
- IPv6 routing protocols: IS-IS for IPv6, IPv6 BGP

[Table 34 on page 240](#) lists the AFLs that you can purchase for EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 switches. If you have the license, you can run all of the advanced software features mentioned above on your EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, or EX9200 switch.

Table 44: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches

Switch Model	AFL Part Number
EX3200-24P EX3200-24T EX4200-24F EX4200-24P EX4200-24PX EX4200-24T	EX-24-AFL
EX3200-48P EX3200-48T EX4200-48F EX4200-48P EX4200-48PX EX4200-48T	EX-48-AFL

Table 44: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches (continued)

Switch Model	AFL Part Number
EX4500-40F-BF EX4500-40F-BF-C EX4500-40F-FB EX4500-40F-FB-C	EX-48-AFL
EX4550	EX4550-AFL
EX6210	EX6210-AFL
EX8208	EX8208-AFL
EX8216	EX8216-AFL
EX-XRE200	EX-XRE200-AFL
EX9204	EX9204-AFL
EX9208	EX9208-AFL
EX9214	EX9214-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4200 and EX4550 switches.

License Warning Messages

For using features that require a license, you must install and configure a license key. To obtain a license key, use the contact information provided in your certificate.

If you have not purchased the AFL or EFL and installed the license key, you receive warnings when you try to commit the configuration:

```
[edit protocols]
  'bgp'
    warning: requires 'bgp' license
error: commit failed: (statements constraint check failed)
```

The system generates system log (**syslog**) alarm messages notifying you that the feature requires a license—for example:

```
Sep 3 05:59:11 craftd[806]: Minor alarm set, BGP Routing Protocol usage
requires a license
Sep 3 05:59:11 alarmd[805]: Alarm set: License color=YELLOW, class=CHASSIS,
reason=BGP Routing Protocol usage requires a license
Sep 3 05:59:11 alarmd[805]: LICENSE_EXPIRED: License for feature bgp(47) expired
```

Output of the **show system alarms** command displays the active alarms:

```
user@switch> show system alarms
1 alarm currently active
Alarm time          Class  Description
2009-09-03 06:00:11 UTC  Minor  BGP Routing Protocol usage requires a license
```

**Related
Documentation**

- *Managing Licenses for the EX Series Switch (CLI Procedure)*
- *Managing Licenses for the EX Series Switch (J-Web Procedure)*
- *Monitoring Licenses for the EX Series Switch*
- *License Key Components for the EX Series Switch*

Installing and Managing Licenses

- [Adding New Licenses \(CLI Procedure\) on page 255](#)
- [Deleting a License \(CLI Procedure\) on page 256](#)
- [Saving License Keys on page 257](#)
- [Verifying Junos OS License Installation on page 258](#)

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 258](#).

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 256](#)
- [Junos OS Feature Licenses on page 221](#)
- [Verifying Junos OS License Installation on page 258](#)
- [request system license add on page 300](#)

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 258.



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 255](#)
- [Saving License Keys on page 257](#)
- [Junos OS Feature Licenses on page 221](#)
- [Verifying Junos OS License Installation on page 258](#)
- [request system license delete on page 301](#)

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 258.

Related Documentation

- [Adding New Licenses \(CLI Procedure\) on page 255](#)
- [Deleting a License \(CLI Procedure\) on page 256](#)
- [Junos OS Feature Licenses on page 221](#)
- [Verifying Junos OS License Installation on page 258](#)

Verifying Junos OS License Installation

To verify Junos OS license management, perform the following tasks:

- [Displaying Installed Licenses on page 258](#)
- [Displaying License Usage on page 259](#)

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:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
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

- [Troubleshooting Software Installation on page 263](#)

Troubleshooting Software Installation

- [Troubleshooting Software Installation on page 263](#)
- [Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 266](#)
- [Disk Space Management for Junos OS Installation on page 267](#)
- [Verifying PIC Combinations on page 267](#)

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 on page 263](#)
- [Rebooting from the Inactive Partition on page 264](#)
- [Freeing Disk Space for Software Installation on page 265](#)
- [Installation from the Boot Loader Generates 'cannot open package' Error on page 265](#)

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 162 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, **ftp://192.171.28/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=diskxy:
```

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 \(CLI Procedure\)](#)
- [Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade \(CLI Procedure\)](#)
- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)
- [show system storage partitions \(EX Series Switches Only\) on page 413](#)

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 131](#)
- [Troubleshooting Software Installation on page 263](#)
- [show system storage partitions \(EX Series Switches Only\) on page 413](#)

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 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.

Related Documentation

- [Junos OS Configuration Using the CLI](#)

Verifying PIC Combinations

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 up to 11 (on SRX5800) and five (SRX5600) SPCs and IOCs on the device. However you must install at least one SPC on device. For more details, see [SRX5600 and SRX5800 Services Gateway Card Guide](#).

For more information about PIC combinations or about unsupported PIC combinations, see the corresponding PIC guide or *Hardware Guide* for your device, and the *Junos OS Release Notes* on the Juniper Networks Support website at <http://www.juniper.net/support/>.

- Related Documentation**
- [Hardware Overview of SRX Series Services Gateways on page 31](#)
 - [Storage Media Names for SRX Series Devices on page 34](#)

PART 5

Configuration Statements and Operational Commands

- Configuration Statements on page 271
- Operational Commands on page 287

CHAPTER 17

Configuration Statements

- auto-configuration on page 272
- auto-configuration (System) on page 273
- auto-image-upgrade on page 275
- auto-snapshot on page 276
- autoinstallation on page 277
- autoinstallation (JNU Satellite Devices) on page 278
- bootp on page 279
- commit on page 280
- configuration-servers on page 281
- delete-after-commit (JNU Satellites) on page 282
- interfaces (Autoinstallation) on page 283
- license on page 284
- usb on page 286
- usb-control on page 286

auto-configuration

Syntax	auto-configuration { command <i>binary-file-path</i> ; disable; }
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Configure the autoconfiguration process.
Options	<ul style="list-style-type: none">• command <i>binary-file-path</i>—Path to the binary process.• disable—Disable the autoconfiguration process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Autoinstallation Overview on page 81• Configuring Autoinstallation on SRX Series Devices on page 84

auto-configuration (System)

Syntax	<pre> auto-configuration { traceoptions { file { filename; files number; match regular-expression; size maximum-file-size; (world-readable no-world-readable); } flag flag; level (all error info notice verbose warning); no-remote-trace; } } </pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the autoconfiguration process.
Options	<p>traceoptions—Set the trace options.</p> <ul style="list-style-type: none"> • file—Configure the trace file information. <ul style="list-style-type: none"> • 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 <code>/var/log</code>. 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 <code>trace-file</code> reaches its maximum size, it is renamed to trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten. <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000 files</p> <p>Default: 10 files</p> • 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). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues 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** option and a filename.

Syntax: x K to specify KB, x m to specify MB, or x g to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **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**—Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.
 - **all**—Trace all events.
 - **auth**—Trace VLAN authentication.
 - **configuration**—Trace configurations.
 - **interfaces**—Trace interface operations.
 - **io**—Trace I/O operations.
 - **rtsock**—Trace routing socket operations.
 - **ui**—Trace user interface operations.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Autoinstallation Overview on page 81](#)
- [Configuring Autoinstallation on SRX Series Devices on page 84](#)

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	<p>Enable automatic software download on an EX Series switch acting as a DHCP client.</p> <p>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.</p> <p>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.</p>
Default	Automatic software download is disabled.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Upgrading Software by Using Automatic Software Download on page 129 • Understanding Software Installation on EX Series Switches on page 44 • 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.
<hr/>	
	 NOTE: EX9200 switches do not support the automatic snapshot feature.
<hr/>	
Default	<ul style="list-style-type: none">• The automatic snapshot feature is enabled by default on the following EX Series switches:<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Understanding Resilient Dual-Root Partitions on Switches on page 95• show system auto-snapshot on page 392

autoinstallation

Syntax	<pre>autoinstallation { configuration-servers { url { password <i>password</i>; } } interfaces { <i>interface-name</i> { bootp; rarp; } } usb { disable; } }</pre>
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. See CLI Explorer .
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Autoinstallation on SRX Series Devices on page 84

autoinstallation (JNU Satellite Devices)

Syntax	<pre>autoinstallation { delete-after-commit; configuration-servers { url; } interfaces { interface-name { bootp; rarp; } } }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 13.3 for satellite devices in a Junos Node Unifier (JNU) group.
Description	(Satellite devices in a JNU group). Download a configuration file automatically from an FTP or HTTP server. When you power on a router or switch configured for autoinstallation, it requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server. When the router or switch has an address, it sends a request to a configuration server and downloads and installs a configuration.
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	<ul style="list-style-type: none">• Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91• Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89• Configuring Autoinstallation on JNU Satellite Devices on page 87• Verifying Autoinstallation on JNU Satellite Devices on page 92• delete-after-commit (JNU Satellites) on page 282• configuration-servers

bootp

Syntax	<pre>bootp { command <i>binary-file-path</i>; disable; failover (alternate-media other-routing-engine); }</pre>
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the booting process.
Options	<ul style="list-style-type: none">• command <i>binary-file-path</i>—Path to the binary process.• disable —Disable the booting process.• failover—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.<ul style="list-style-type: none">• alternate-media—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.• other-routing-engine—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">•

commit

Syntax	<pre>commit { server { commit-interval <i>seconds</i>; days-to-keep-error-logs <i>days</i>; maximum-aggregate-pool <i>number</i>; maximum entries <i>number</i>; traceoptions { file { <i>filename</i>; files <i>number</i>; microsecond-stamp; size <i>maximum-file-size</i>; (world-readable no-world-readable); } flag <i>flag</i>; no-remote-trace; } } synchronize; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	Configure the commit operation.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><i>Controlling Execution of Commit Scripts During Commit Operations</i>

configuration-servers

Syntax	<pre>configuration-servers { url { password <i>password</i>; } }</pre>
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure the URL address of a server from which the configuration files must be obtained.</p> <p>You can download a configuration file automatically from an FTP, Hypertext Transfer Protocol (HTTP), or Trivial FTP (TFTP) servers. Examples of URLs:</p> <ul style="list-style-type: none">• <code>tftp://hostname/path/filename</code>• <code>ftp://username:password@ftp.hostname.net</code>• <code>http://hostname/path/filename</code>• <code>http://username:password@httpconfig.sp.com</code>
Options	<ul style="list-style-type: none">• url—Specify the URL address of the server containing the configuration files.• password—Specify the password for authentication with the configuration server. Specifying a password in URLs and in the <i>password</i> option might result in commit failure. We recommend you to use the <i>password</i> option for specifying the password.
Required Privilege Level	<p><code>system</code>—To view this statement in the configuration.</p> <p><code>system-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Autoinstallation on SRX Series Devices on page 84

delete-after-commit (JNU Satellites)

Syntax	delete-after-commit;
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced in Junos OS Release 13.3 for satellite devices in a Junos Node Unifier (JNU) group.
Description	Specify that during the subsequent commit operation of configuration settings (after the autoinstallation process successfully retrieves, installs, and commits the configuration), the autoinstallation configuration parameters be removed from the router. Removal of the autoinstallation parameters and statements from the committed configuration on the router ensures that the router does not attempt to perform an autoinstallation process when it is powered on the next time. Although you can optionally specify the interfaces to perform autoinstallation or configuration servers from which the files are to be downloaded, you must include the delete-after-commit statement to prevent the router from entering a recursive loop and repeatedly performing an autoinstallation every time it is powered on.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91• Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89• Configuring Autoinstallation on JNU Satellite Devices on page 87• Verifying Autoinstallation on JNU Satellite Devices on page 92• autoinstallation on page 278• configuration-servers

interfaces (Autoinstallation)

Syntax	<pre> interfaces { interface-name { bootp; rarp; } } </pre>
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.
	<p> NOTE: When you run the system autoinstallation command, the command will configure unit 0 logical interface for all the active state physical interfaces. However, few commands like fabric-options do not allow its physical interface to be configured with a logical interface. If the system autoinstallation and the fabric-options commands are configured together the following message is displayed incompatible with 'system autoinstallation'.</p>
Options	<ul style="list-style-type: none"> • bootp—Enables BOOTP or DHCP during autoinstallation. • rarp—Enables RARP during autoinstallation.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Autoinstallation Overview on page 81 • Configuring Autoinstallation on SRX Series Devices on page 84

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 Feature License Keys*

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	<ul style="list-style-type: none">• Configuring Autoinstallation on SRX Series Devices on page 84

usb-control

Syntax	usb-control { command <i>binary-file-path</i> ; disable; }
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the universal serial bus (USB) supervise process.
Options	<ul style="list-style-type: none">• command <i>binary-file-path</i>—Path to the binary process.• disable—Disable the universal serial bus (USB) supervise process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

CHAPTER 18

Operational Commands

- clear system login lockout
- request system autorecovery state
- request system download abort
- request system download clear
- request system download pause
- request system download resume
- request system download start
- request system firmware upgrade
- request system halt
- request system license add
- request system license delete
- request system license save
- request system license update
- request system partition compact-flash
- request system power-off
- request system reboot
- request system reboot
- request system reboot (Junos OS with Upgraded FreeBSD)
- request system scripts add
- request system scripts delete
- request system scripts rollback
- request system snapshot
- request system snapshot (Junos OS with Upgraded FreeBSD)
- request system snapshot (SRX Series)
- request system software abort in-service-upgrade (ICU)
- request system software add
- request system software add (Maintenance)
- request system software configuration-backup

- request system software configuration-restore
- request system software delete
- request system software rollback
- request system software rollback (SRX Series)
- request system software validate
- request system software validate on (Junos OS with Upgraded FreeBSD)
- request system storage cleanup
- request system storage cleanup (SRX Series)
- request system zeroize
- show chassis usb storage
- 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 (View)
- show system login lockout
- show system snapshot
- show system snapshot (Junos OS with Upgraded FreeBSD)
- show system snapshot media
- 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 <i>username</i> >
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 <i>username</i> —Clear the specified locked user account.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• <i>lockout-period</i>• show system login lockout on page 407
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 OS Release 11.2.
Description	Prepare the system for autorecovery of configuration, licenses, and disk information.
Options	<p>save—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.</p> <p>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.</p>
	<p> NOTE:</p> <ul style="list-style-type: none"> 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.
	<p>recover—Recover the disk partitioning, configuration, and licenses.</p> <p>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.</p>
	<p>clear—Clear all saved autorecovery information.</p> <p>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.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> show system autorecovery state on page 383
List of Sample Output	<ul style="list-style-type: none"> request system autorecovery state save on page 291 request system autorecovery state recover on page 291 request system autorecovery state clear on page 291
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 bsdlablel 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 bsdlablel recovery information
```

request system download abort

Syntax request system download abort <*download-id*>

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

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 system download** command until a **request system download 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 aborted.

Required Privilege Level maintenance

Related Documentation

- [request system download start on page 296](#)
- [request system download pause on page 294](#)
- [request system download resume on page 295](#)
- [request system download clear on page 293](#)

List of Sample Output [request system download abort on page 292](#)

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 Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Delete the history of completed and aborted downloads.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 296• request system download pause on page 294• request system download resume on page 295• request system download abort on page 292
List of Sample Output	request system download clear on page 293
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 Junos OS Release 11.2.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

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 296](#)
- [request system download resume on page 295](#)
- [request system download abort on page 292](#)
- [request system download clear on page 293](#)

List of Sample Output [request system download pause on page 294](#)

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	<code>request system download resume <i>download-id</i> <max-rate></code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
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.
<hr/>  NOTE: Only downloads in the paused and error states can be resumed. <hr/>	
Options	<p>download-id—(Required) The ID number of the download to be resumed.</p> <p>max-rate—(Optional) The maximum bandwidth for the download.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system download start on page 296 • request system download pause on page 294 • request system download abort on page 292 • request system download clear on page 293
List of Sample Output	request system download resume on page 295
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	<code>request system download start (url max-rate save as login delay)</code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Creates a new download instance and identifies it with a unique integer called the download ID.
Options	<p>url—(Required) The FTP or HTTP URL location of the file to be downloaded.</p> <p>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.</p> <p>save-as—(Optional) The filename to be used for saving the file in the <code>/var/tmp</code> location.</p> <p>login—(Optional) The username and password for the server in the format <code>username:password</code>.</p> <p>delay—(Optional) The number of hours after which the download should start.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download pause on page 294• request system download resume on page 295• request system download abort on page 292• request system download clear on page 293
List of Sample Output	request system download start on page 296
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 Junos OS Release 10.2.
Description	Upgrade firmware on a system.
Options	<p>fpc—Upgrade FPC ROM monitor.</p> <p>pic—Upgrade PIC firmware.</p> <p>re—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.</p> <p>vcpu—Upgrade VCPU ROM monitor.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system license update on page 303
List of Sample Output	request system firmware upgrade on page 297
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 halt

Syntax	request system halt at < <i>time</i> > in < <i>minutes</i> > media (compact-flash disk usb) messages < <i>message</i> >
Release Information	Command introduced in Junos OS Release 11.4.
Description	Stop the system.
Options	<p>at <i>time</i>— Time at which to stop the system.</p> <p>in <i>minutes</i>— Number of minutes to delay before halting the system.</p> <p>media —Boot media for the next boot.</p> <ul style="list-style-type: none"> • compact-flash— Standard boot from a flash device. • disk— Boot from a hard disk. • usb— Boot from a USB device. <p>message <i>message</i>— Message that is displayed to all system users before stopping the system.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system power-off on page 305
List of Sample Output	request system halt on page 298
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system halt

```

user@host> request system halt
Halt the system ? [yes,no] (no) yes

*** FINAL System shutdown message from root@quickland ***

System going down IMMEDIATELY

Shutdown NOW!
[pid 7560]

root@quickland> Dec  8 08:57:37 Waiting (max 60 seconds) for system process `vn1ru'
to stop...done
Waiting (max 60 seconds) for system process `vn1ru_mem' to stop...done

```

```
Waiting (max 60 seconds) for system process `bufdaemon' to stop...done
Waiting (max 60 seconds) for system process `syncer' to stop...
Syncing disks, vnodes remaining...2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 0 0 0 0 0 0
0 0 0 0 0 done
```

```
syncing disks... All buffers synced.
Uptime: 2d16h25m9s
recorded reboot as normal shutdown
```

```
The operating system has halted.
Please press any key to reboot.
```

request system license add

Syntax	<code>request system license add (filename terminal)</code>
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	<ul style="list-style-type: none">• Adding New Licenses (CLI Procedure) on page 255
List of Sample Output	request system license add on page 300
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 qcsbj a okbuqe rcmxnq vjocwf uxfsta
          z5ufjb kdrmt6 57bimv 2f3ddp qttdcn 627q4a
          jx4s5x hiri
E408408918: successfully added
add license complete (no errors)
```

request system license delete

Syntax	<code>request system license delete (<i>license-identifier</i> license-identifier-list [<i>licenseid001 licenseid002 licenseid003</i>] all)</code>
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	<i>license-identifier</i> —Text string that uniquely identifies a license key. license-identifier-list [<i>licenseid001 licenseid002 licenseid003....</i>] —Delete multiple license identifiers as a list enclosed in brackets. all —Delete all licenses on the device.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• Deleting a License (CLI Procedure) on page 256

request system license save

Syntax	request system license save (<i>filename</i> 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	<ul style="list-style-type: none">• Saving License Keys on page 257
List of Sample Output	request system license save on page 302
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 Junos OS Release 9.5.
Description	Start autoupdating license keys from the LMS server.
Options	trial —Starts autoupdating trial license keys from the LMS server.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • show system license (View) on page 404
List of Sample Output	request system license update on page 303 request system license update trial on page 303
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
```

```
Request to automatically 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 Junos OS Release 9.2. Command deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.
	<p> NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “Understanding Junos OS with Upgraded FreeBSD” on page 19.</p>
Description	Reboots the device and repartitions the compact flash. The CompactFlash card is repartitioned only if it is possible to restore all the data on the CompactFlash card. 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 304 request system partition compact-flash (If No) on page 304
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 power-off

Syntax	request system power-off at < <i>time</i> > in < <i>minutes</i> > media (compact-flash disk usb) messages < <i>message</i> >
Release Information	Command introduced in Junos OS Release 11.4.
Description	Power off the system.
Options	<p>at <i>time</i>— Time at which to power off the system.</p> <p>in <i>minutes</i>— Number of minutes to delay before powering off the system.</p> <p>media —Boot media for the next boot.</p> <ul style="list-style-type: none"> • compact-flash— Standard boot from a flash device. • disk— Boot from a hard disk. • usb— Boot from a USB device. <p>message <i>message</i>— Message that is displayed to all system users before powering off the system.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system halt on page 298
List of Sample Output	request system power-off on page 305
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system power-off

```

user@host> request system power-off
Power Off the system ? [yes,no] (no) yes

Shutdown NOW!
[pid 3300]

*** FINAL System shutdown message from root@quickland ***

System going down IMMEDIATELY

root@quickland> Dec  8 09:37:45 Waiting (max 60 seconds) for system process `vn1ru'
to stop...done
Waiting (max 60 seconds) for system process `vn1ru_mem' to stop...done

```

```
Waiting (max 60 seconds) for system process `bufdaemon' to stop...done
Waiting (max 60 seconds) for system process `syncer' to stop...
Syncing disks, vnodes remaining...2 2 2 2 2 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0
0 0 0 0 done
```

```
syncing disks... All buffers synced.
Uptime: 38m33s
recorded reboot as normal shutdown
```

```
The operating system has halted.
Turning the system power off.
```

request system reboot

List of Syntax	Syntax on page 307 Syntax (EX Series Switches) on page 307 Syntax (TX Matrix Router) on page 307 Syntax (TX Matrix Plus Router) on page 307 Syntax (MX Series Router) on page 307
Syntax	<pre>request system reboot <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk removable-compact-flash usb)> <message "<i>text</i>"> <other-routing-engine></pre>
Syntax (EX Series Switches)	<pre>request system reboot <all-members> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <local> <media (external internal)> <member <i>member-id</i>> <message "<i>text</i>"> <other-routing-engine> <slice <i>slice</i>></pre>
Syntax (TX Matrix Router)	<pre>request system reboot <all-chassis all-lcc lcc <i>number</i> scc> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk)> <message "<i>text</i>"> <other-routing-engine></pre>
Syntax (TX Matrix Plus Router)	<pre>request system reboot <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i>> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk)> <message "<i>text</i>"> <other-routing-engine> <partition (1 2 alternate)></pre>
Syntax (MX Series Router)	<pre>request system reboot <all-members> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <local></pre>

```

<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 and TX 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)—(Optional) Boot medium for next boot.

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 311](#)
- [request system reboot \(at 2300\) on page 311](#)
- [request system reboot \(in 2 Hours\) on page 311](#)
- [request system reboot \(Immediately\) on page 311](#)
- [request system reboot \(at 1:20 AM\) on page 311](#)

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	<pre>request system reboot <all-members local member member-id> <at time> <in minutes> <media (external internal)> <message "text"> <slice (1 2 alternate)></pre>
Release Information	<p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Option partition changed to slice in Junos OS Release 10.0 for EX Series switches.</p>
Description	<p>Reboot the Junos OS.</p> <p>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.</p>
Options	<p>none—Reboots the software immediately.</p> <p>all-members local member member-id—(Optional) Specify which member of the Virtual Chassis to reboot:</p> <ul style="list-style-type: none"> • 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. <p>at time—(Optional) Time at which to reboot the software, specified in one of the following ways:</p> <ul style="list-style-type: none"> • +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. <p>in minutes—(Optional) Number of minutes from now to reboot the software. This option is an alias for the at +minutes option.</p> <p>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.</p> <p>message "text"—(Optional) Message to display to all system users before rebooting the software.</p>

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 reboot (Junos OS with Upgraded FreeBSD)

Syntax request system reboot
<all-members>
<at *time*>
<both-routing-engines>
<in *minutes*>
<local>
<media (oam | junos | network | usb)>
<member *member-id*>
<message "*text*">
<other-routing-engine>

Release Information Command introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers and EX9200 switches.
Command introduced in Junos OS Release 15.1X53-D30 for QFX5200 switches.

Description Reboot the software.

Options **none**—Reboot the software immediately.

all-members—(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. Omitting a value will default to the current date for that value.
- ***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.

local—(Optional) Reboot the software on the local Virtual Chassis member.

media (oam | junos | network | usb)—(Optional) Reboot the boot media:

- **oam**—Reboot from the **oam** volume.
- **junos**—Reboot from the **junos** volume.
- **network**—Reboot from the network.
- **usb**—Reboot from the USB device.

member *member-id*—(Optional) Reboot the software on the specified member of the Virtual Chassis configuration. 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.

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*).



NOTE: To reboot a router or switch 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

- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 327](#)
- [show system snapshot \(Junos OS with Upgraded FreeBSD\) on page 411](#)
- [clear system reboot](#)
- [request system halt](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)

List of Sample Output

- [request system reboot on page 315](#)
- [request system reboot \(at 2300\) on page 315](#)
- [request system reboot \(in 2 Hours\) on page 316](#)
- [request system reboot \(Immediately\) on page 316](#)
- [request system reboot \(at 1:20 AM\) on page 316](#)

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 318](#)
- [request system scripts rollback on page 319](#)
- [request system scripts event-scripts](#)

request system scripts delete

Syntax	<code>request system scripts delete <package-name></code>
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	<ul style="list-style-type: none">• request system scripts add on page 317• request system scripts rollback on page 319• <i>request system scripts event-scripts</i>

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	<ul style="list-style-type: none">• request system scripts add on page 317• request system scripts delete on page 318• <i>request system scripts event-scripts</i>

request system snapshot

List of Syntax	<p>Syntax on page 320</p> <p>Syntax (ACX Series Routers) on page 320</p> <p>Syntax (EX Series Switches) on page 320</p> <p>Syntax (MX Series Routers) on page 320</p> <p>Syntax (TX Matrix Routers) on page 320</p> <p>Syntax (TX Matrix Plus Routers) on page 320</p>
Syntax	<pre>request system snapshot <partition></pre>
Syntax (ACX Series Routers)	<pre>request system snapshot <media type> <partition></pre>
Syntax (EX Series Switches)	<pre>request system snapshot <all-members local member member-id> <media type> <partition> <re0 re1 routing-engine routing-engine-id> <slice alternate></pre>
Syntax (MX Series Routers)	<pre>request system snapshot <all-members> <config-partition> <local> <member member-id> <media usb-port-number> <partition> <root-partition></pre>
Syntax (TX Matrix Routers)	<pre>request system snapshot <all-chassis all-lcc lcc number scc> <config-partition> <partition> <root-partition></pre>
Syntax (TX Matrix Plus Routers)	<pre>request system snapshot <all-chassis all-lcc lcc number sfc number> <config-partition> <partition> <root-partition></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 10.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 12.2 for ACX Series switches.</p> <p>Options <config-partition> and <root-partition> introduced in Junos OS Release 13.1 for M, MX, T, TX Series switches.</p> <p>Option media usb-port-number introduced in Junos OS Release 13.2 for MX104 routers.</p> <p>Options <config-partition>, <root-partition>, and <slice> deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.</p>



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in [“Understanding Junos OS with Upgraded FreeBSD” on page 19](#).

- 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 95](#).

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.

Option deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

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.

Option deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

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.

Option deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

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

- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 327](#)
- [show system snapshot on page 408](#)
- [show system auto-snapshot on page 392](#)

List of Sample Output

[request system snapshot \(Routers\) on page 325](#)
[request system snapshot \(EX Series Switches\) on page 325](#)
[request system snapshot \(When the Partition Flag Is On\) on page 325](#)
[request system snapshot \(MX104 routers when media device is missing\) on page 325](#)
[request system snapshot \(When Mirroring Is Enabled\) on page 325](#)
[request system snapshot all-lcc \(Routing Matrix\) on page 325](#)

[request system snapshot all-members \(Virtual Chassis\) on page 326](#)

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 (Junos OS with Upgraded FreeBSD)

Syntax	request system snapshot <delete <i>snapshot-name</i> > <load <i>snapshot-name</i> > <media <i>type</i> > <recovery>
Release Information	Command introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers and EX9200 switches. Command introduced in Junos OS Release 15.1X53-D30 for QFX5200 switches.
Description	On the router or switch, back up the currently running and active file system partitions to standby partitions that are not running. Non-recovery snapshots are named snap.date.time and stored in the /packages/sets directory.
	
<p>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.</p>	
Options	<p>none—On the router or switch, back up the currently running and active file system partitions to standby partitions that are not running. Specifically, this creates a non-recovery snapshot named snap.<date>.<time> which is stored in /packages/sets.</p> <p>delete <i>snapshot-name</i>—(Optional) Delete a specific non-recovery snapshot from /packages/sets. Wildcards are supported, so request system snapshot delete snap* deletes all snapshots.</p> <p>load <i>snapshot-name</i>—(Optional) Load a specific snapshot from /packages/sets.</p> <p>media <i>type</i>—(Optional) Specify the boot device the software is copied to:</p> <ul style="list-style-type: none"> • usb—(MX960 routers only) Copy software to the device connected to the USB port. <p>recovery—Create a recovery snapshot and store it in the /oam volume.</p>
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 /packages/sets file systems. 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 /packages/sets file systems.
Required Privilege Level	maintenance

- Related Documentation**
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 314](#)
 - [show system snapshot \(Junos OS with Upgraded FreeBSD\) on page 411](#)
 - [Understanding Junos OS with Upgraded FreeBSD on page 19](#)

- List of Sample Output**
- [request system snapshot recovery on page 328](#)
 - [request system snapshot delete on page 328](#)
 - [request system snapshot on page 328](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system snapshot recovery

```
user@host> request system snapshot recovery
Creating image ...
Compressing image . . .
Image size is 777MB

Recovery snapshot created successfully
```

request system snapshot delete

```
user@host> request system snapshot delete snap.20150112.122106
NOTICE: Snapshot 'snap.20150112.122106' deleted successfully
```

request system snapshot

```
user@host> request system snapshot
NOTICE: Snapshot snap.20150119.122106 created successfully
```

request system snapshot (SRX Series)

Syntax request system snapshot
 <factory>
 <media (compact-flash | hard-disk | internal | usb)>
 <node (all | local | node-id | primary)>
 <partition>
 <slice (alternate) >

Release Information Command introduced in Junos OS Release 10.2.

Description Back up the currently running and active file system partitions on the device.

- Options**
- **media—** (Optional) Specifies the media to be included in the snapshot:
 - **compact-flash—** Copies the snapshot to the CompactFlash card.
 - **hard-disk—** Copies the snapshot to the hard disk.
 - **usb—** Copies the snapshot to the USB storage device.
 - **node—** (Optional) Specifies the archive data and executable areas of a specific node.
 - **node-id—** Specifies for node(0, 1).
 - **all—** Specifies for all nodes.
 - **local—** Specifies for local nodes.
 - **primary—** Specifies for primary nodes.
 - **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.

Example: request system snapshot media usb partition

Example: request system snapshot media usb partition factory

- **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	<ul style="list-style-type: none">• Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110
List of Sample Output	request system snapshot media hard-disk on page 330 request system snapshot media usb (when usb device is missing on page 330 request system snapshot media compact-flash on page 330 request system snapshot partition on page 330
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request system snapshot media hard-disk](#)

```
user@host> request system snapshot media hard-disk
Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...
```

[request system snapshot media usb \(when usb device is missing](#)

```
user@host> request system snapshot media usb
Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media / partition (da1s1a)...
Running newfs (47MB) on usb media /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

[request system snapshot media compact-flash](#)

```
user@host> request system snapshot media compact-flash
error: cannot snapshot to current boot device
```

[request system snapshot partition](#)

```
user@host> request system snapshot partition
Verifying compatibility of destination media partitions...
Running newfs (439MB) on internal media / partition (da0s1a)...
Running newfs (46MB) on internal media /config partition (da0s1e)...
Copying '/dev/da1s1a' to '/dev/da0s1a' .. (this may take a few minutes)
Copying '/dev/da1s1e' to '/dev/da0s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system software abort in-service-upgrade (ICU)

Syntax	request system software abort in-service-upgrade
Release Information	Command introduced in Junos OS Release 11.2.
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	<ul style="list-style-type: none">• <i>request system software in-service-upgrade (Maintenance)</i>
List of Sample Output	request system software abort in-service-upgrade on page 331
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 on page 332
 - Syntax (EX Series Switches) on page 332
 - Syntax (TX Matrix Router) on page 332
 - Syntax (TX Matrix Plus Router) on page 333
 - Syntax (MX Series Router) on page 333
 - Syntax (QFX Series) on page 333
 - Syntax (OCX Series) on page 333

Syntax request system software add *package-name*
 <best-effort-load>
 <delay-restart>
 <device-alias *alias-name*>
 <force>
 <no-copy>
 <no-validate>
 <re0 | re1>
 <reboot>
 <satellite *slot-id*>
 <set [*package-name package-name*]>
 <unlink>
 <upgrade-group [all |*upgrade-group-name*]>
 <upgrade-with-config>
 <upgrade-with-config-format *format*>
 <satellite *slot-id*>
 <validate>
 <version *version-string*>

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>

	<pre> <upgrade-with-config-format <i>format</i>> <validate> </pre>
Syntax (TX Matrix Plus Router)	<pre> request system software add <i>package-name</i> <best-effort-load> <delay-restart> <force> <lcc <i>number</i> sfc <i>number</i>> <no-copy> <no-validate> <re0 re1> <reboot> <set [<i>package-name package-name</i>]> <unlink> <upgrade-with-config> <upgrade-with-config-format <i>format</i>> <validate> </pre>
Syntax (MX Series Router)	<pre> request system software add <i>package-name</i> <best-effort-load> <delay-restart> <device-alias <i>alias-name</i>> <force> <member <i>member-id</i>> <no-copy> <no-validate> <re0 re1> <reboot> <satellite <i>slot-id</i>> <set [<i>package-name package-name</i>]> <upgrade-group [all <i>upgrade-group-name</i>]> <unlink> <upgrade-with-config> <upgrade-with-config-format <i>format</i>> <validate> <version <i>version-string</i>> </pre>
Syntax (QFX Series)	<pre> request system software add <i>package-name</i> <best-effort-load> <component all> <delay-restart> <force> <force-host> <no-copy> <no-validate> <partition> <reboot> <unlink> <upgrade-with-config> <upgrade-with-config-format <i>format</i>> <validate> </pre>
Syntax (OCX Series)	<pre> request system software add <i>package-name</i> <best-effort-load> <delay-restart> </pre>

```

<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.

device-alias, **satellite**, **upgrade-group**, and **version** options introduced in Junos OS Release 14.2R3 for Junos Fusion.

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 OS.



NOTE: When graceful Routing Engine switchover (GRES) is enabled on a device, you must perform a unified ISSU operation to update the software running on the device. With GRES enabled, if you attempt to perform a software upgrade by entering the request system software add *package-name* command, an error message is displayed stating that only in-service-software-upgrades are supported when GRES is configured. In such a case, you must either remove the GRES configuration before you attempt the upgrade or perform a unified ISSU.

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`

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.

device-alias *alias-name*—(Junos Fusion only) (Optional) Install the satellite software package onto the specified satellite device using the satellite device's alias name.

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.

satellite *slot-id*—(Junos Fusion only) (Optional) Install the satellite software package onto the specified satellite device using the satellite devices FPC slot identifier.

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 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-group [all [*upgrade-group-name*]—(Junos Fusion only) (Required to configure a Junos Fusion using autoconversion or manual conversion) Associate a satellite software image with a satellite software upgrade group. The satellite software package is associated with the specified satellite software upgrade group using the

upgrade-group-name, or for all satellite software upgrade groups in a Junos Fusion when the all keyword is specified.

A satellite software upgrade group is a group of satellite devices in a Junos Fusion that are designated to upgrade to the same satellite software version using the same satellite software package. See *Understanding Software in a Junos Fusion* and *Managing Satellite Software Upgrade Groups in a Junos Fusion*.

upgrade-with-config—(Optional) Install one or more configuration files.

upgrade-with-config-format *format*—(Optional) Specify the configuration file format, **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.

version *version-string*—(Junos Fusion only) (Optional) Associate a satellite software package with a satellite software upgrade group by selecting the satellite software package's version. This option can only be used if the specified version of the satellite software has previously been installed on the aggregation device.

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, **jkernl**, last. Add the operating system package, **jkernl**, 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/jkernl
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 345](#)
- [request system software rollback on page 349](#)
- [request system storage cleanup on page 362](#)
- [Upgrading Software](#)
- [Upgrading Software on a QFabric System](#)
- [Managing Satellite Software Upgrade Groups in a Junos Fusion](#)
- [request system software add \(Maintenance\) on page 342](#)

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [request system software add validate on page 340](#)
[request system software add \(Mixed EX4200 and EX4500 Virtual Chassis\) on page 341](#)
[request system software add component all \(QFabric Systems\) on page 341](#)
[request system software add upgrade-group \(Junos Fusion\) on page 341](#)

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 upgrade-group (Junos Fusion)

```
user@aggregation-device> request system software add /var/tmp/satellite-1.0R1.1-signed.tgz
upgrade-group group1
```

request system software add (Maintenance)

Syntax	<code>request system software add <i>package-name</i></code>
Release Information	Partition option introduced in the command in Junos OS Release 10.1.
Description	Install the new software package on the device. For example: request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot.
Options	<ul style="list-style-type: none">• <code>delay-restart</code> — Installs the software package but does not restart the software process• <code>best-effort-load</code> — Activate a partial load and treat parsing errors as warnings instead of errors• <code>no-copy</code> — Installs the software package but does not saves the copies of package files• <code>no-validate</code> — Does not check the compatibility with current configuration before installation starts• <code>partition</code> — Formats and re-partitions the media before installation• <code>reboot</code> — Reboots the device after installation is completed• <code>unlink</code> — Removes the software package after successful installation• <code>validate</code> — Checks the compatibility with current configuration before installation starts
Required Privilege Level	<code>maintenance</code>
Related Documentation	<ul style="list-style-type: none">• <code>request system reboot</code>

request system software configuration-backup

Syntax	request system software configuration-backup (<i>path</i>)
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	<ul style="list-style-type: none"> • request system software configuration-restore on page 344 • <i>Performing a QFabric System Recovery Installation on the Director Group</i>
List of Sample Output	request system software configuration-backup on page 343
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 (<i>path</i>)
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	<ul style="list-style-type: none"> • request system software configuration-backup on page 343 • <i>Performing a QFabric System Recovery Installation on the Director Group</i>
List of Sample Output	request system software configuration-restore on page 344
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 345 Syntax (TX Matrix Router) on page 345 Syntax (TX Matrix Plus Router) on page 345
Syntax	<pre>request system software delete <i>software-package</i> <force> <reboot> <set [<i>package-name package-name</i>]> <upgrade-group [<i>all upgrade-group-name</i>]> <version <i>version-string</i>></pre>
Syntax (TX Matrix Router)	<pre>request system software delete <i>software-package</i> <force> <lcc <i>number</i> <i>scc</i>> <reboot> <set [<i>package-name package-name</i>]></pre>
Syntax (TX Matrix Plus Router)	<pre>request system software delete <i>software-package</i> <force> <lcc <i>number</i> <i>sfc number</i>> <reboot> <set [<i>package-name package-name</i>]></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Option sfc introduced for the TX Matrix Plus router in Junos OS Release 9.6.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Option set [<i>package-name package-name</i>] added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Services Gateways.</p> <p>Option reboot introduced in Junos OS Release 12.3.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Options upgrade-group, and version introduced in Junos OS Release 14.2R3 for Junos Fusion.</p>
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

- **jkern**—(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) In a routing matrix, delete a software package or bundle on a T640 router indicated by **lcc number** that is connected to the TX Matrix router. In a routing matrix, delete a software package or bundle on a router indicated by **lcc number** 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.

re0 | re1—(Optional) On routers or switches that support dual or redundant Routing Engines, delete a software package or bundle on the Routing Engine in slot 0 (re0) or the Routing Engine in slot 1 (re1).

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.

upgrade-group [all [*upgrade-group-name*]]—(Junos Fusion only) Delete the satellite software image association with the specified satellite software upgrade group.

A satellite software upgrade group is a group of satellite devices in the same Junos Fusion that are designated to upgrade to the same satellite software version using the same satellite software package.

version *version-string*—(Junos Fusion only) (Optional) Delete a satellite software package association with a satellite software upgrade group by selecting the satellite software package's version.

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 332](#)
- [request system software rollback on page 349](#)
- [request system software validate on page 355](#)
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [request system software delete jdocs on page 347](#)

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 rollback

List of Syntax	<p>Syntax on page 349</p> <p>Syntax (EX Series Switches) on page 349</p> <p>Syntax (TX Matrix Router) on page 349</p> <p>Syntax (TX Matrix Plus Router) on page 349</p> <p>Syntax (MX Series Router) on page 349</p>
Syntax	request system software rollback
Syntax (EX Series Switches)	<pre>request system software rollback <all-members> <local> <member member-id> <reboot></pre>
Syntax (TX Matrix Router)	<pre>request system software rollback <lcc number scc> <reboot></pre>
Syntax (TX Matrix Plus Router)	<pre>request system software rollback <lcc number sfc number> <reboot></pre>
Syntax (MX Series Router)	<pre>request system software rollback <all-members> <device-alias alias-name> <local> <member member-id> <reboot> <satellite slot-id> <upgrade-group [all upgrade-group-name]></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Option sfc introduced for the TX Matrix Plus router in Junos OS Release 9.6.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command behavior changed in Junos OS Release 12.1.</p> <p>Option reboot introduced in Junos OS Release 12.3.</p> <p>Options device-alias, satellite, and upgrade-group introduced in Junos OS Release 14.2R3 for Junos Fusion.</p> <p>Option force deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.</p>



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

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 **bundle** package containing the required package) cannot be found in `/var/sw/pkg`.

Additional Information

- On a Junos Fusion, the **request system software rollback** command can be used to roll back the version of satellite software associated with a satellite software upgrade group. Rolling back the version of satellite software associated with a satellite software upgrade group triggers a satellite software upgrade.
- 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. Roll back 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.

device-alias alias-name—(Junos Fusion only) (Optional) Rollback the satellite software package onto the specified satellite device using the satellite devices FPC slot identifier.

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.

satellite *slot-id*—(Junos Fusion only) (Optional) Roll back the satellite software package onto the specified satellite device using the satellite devices FPC slot identifier.

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.

upgrade-group [all [*upgrade-group-name*]]—(Junos Fusion only) Roll back the satellite software image associated with the specified satellite software upgrade group, or for all satellite software upgrade groups in the Junos Fusion when **all** is entered.

Required Privilege Level maintenance

Related Documentation

- [request system software abort](#)
- [request system software add on page 332](#)
- [request system software delete on page 345](#)
- [request system software validate on page 355](#)

- *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 353](#)

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 (SRX Series)

Syntax	<code>request system software rollback <node-id></code>
Release Information	Command introduced in Junos OS Release 10.1. Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.
Description	Revert to the software that was loaded at the last successful request system software add command. Example: request system software rollback .
Options	<i>node-id</i> —Identification number of the chassis cluster node. It can be 0 or 1.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>request system reboot</i>

request system software validate

List of Syntax	Syntax 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	<pre>request system software validate <i>package-name</i> <set [<i>package-name package-name</i>]> <upgrade-with-config> <upgrade-with-config-format <i>format</i>></pre>
Syntax (TX Matrix Router)	<pre>request system software validate <i>package-name</i> <lcc <i>number</i> <i>scc</i>> <set [<i>package-name package-name</i>]> <upgrade-with-config> <upgrade-with-config-format <i>format</i>></pre>
Syntax (TX Matrix Plus Router)	<pre>request system software validate <i>package-name</i> <lcc <i>number</i> <i>sfc number</i>> <set [<i>package-name package-name</i>]> <upgrade-with-config> <upgrade-with-config-format <i>format</i>></pre>
Syntax (MX Series Router)	<pre>request system software validate <i>package-name</i> <member <i>member-id</i>> <set [<i>package-name package-name</i>]> <upgrade-with-config> <upgrade-with-config-format <i>format</i>></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>set [<i>package-name package-name</i>] option added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways.</p> <p>upgrade-with-config and upgrade-with-config-format <i>format</i> options added in Junos OS Release 12.3 for M Series routers, MX Series routers, and T Series routers.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Validate candidate software against the current configuration of the router.
Options	<p>lcc <i>number</i>—(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.</p>

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 format, **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 332](#)
- [request system software delete on page 345](#)
- [request system software rollback on page 349](#)
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [request system software validate \(Successful Case\) on page 357](#)
[request system software validate \(Failure Case\) on page 357](#)

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 software validate on (Junos OS with Upgraded FreeBSD)

Syntax (MX240, MX480, MX960, MX2010, MX2020 Routers only)	request system software validate on <host <i>host-name</i> [username <i>user-name</i>]> <routing-engine (re0 re1)>
Release Information	Command introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, MX2020 routers only.
Description	<p>Direct validation of a running configuration is not possible on a device running Junos OS with upgraded FreeBSD. Nevertheless, validation is an important step in the installation of an upgraded operating system. This command allows validation on a device that is not running Junos OS with upgraded FreeBSD.</p> <p>This command validates the current configuration on a Routing Engine that is not running Junos OS with upgraded FreeBSD or a remote host.</p>
Options	<p>The specific options available are:</p> <p>host <i>host-name</i> [username <i>user-name</i>]—Validate the current configuration on a remote host. The host-name is resolved through DNS. Optionally, you can supply a user-name to employ on the remote host. If you omit the user-name option, the currently logged-in user-name is sent to the remote host.</p> <p>routing-engine (re0 re1)—Validate the current configuration on another Routing Engine on the same device. The other Routing Engine cannot be running Junos OS with upgraded FreeBSD or the validation does not succeed.</p>
Additional Information	If the authenticity of the remote host cannot be established, you are prompted to continue the validation or not. If you choose not to continue, the validation process does not take place.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system reboot (Junos OS with Upgraded FreeBSD) on page 314 • show system snapshot (Junos OS with Upgraded FreeBSD) on page 411 • Understanding Junos OS with Upgraded FreeBSD on page 19
List of Sample Output	request system software validate on host on page 360 request system software validate on routing-engine on page 360
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software validate on host

```
user@host> request system software validate on host remote-validator
The authenticity of host 'remote-validator (192.168.164.174)' can't be established.
ECDSA key fingerprint is 73:d0:78:ce:8d:09:aa:92:4c:ce:45:52:1d:76:86:b5.
Are you sure you want to continue connecting (yes/no)? yes
Password: *****

                Sending /var/tmp/config.tgz to remote-validator...
Validating /var/tmp/config.tgz on remote-validator...
Checking compatibility with configuration
Initializing...
Using jbase-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jruntime-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jkernel-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jroute-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jcrypto-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jweb-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using /var/tmp/config.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: warning: schema: init: 'logical-systems-vlans' contains-node 'juniper-config
  vlans': not found
mgd: commit complete
Validation succeeded
```

request system software validate on routing-engine

```
user@host> request system software validate on routing-engine re1

                Sending /var/tmp/config.tgz to re1...
Validating /var/tmp/config.tgz on re1...
Checking compatibility with configuration
Initializing...
Using jbase-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jruntime-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jkernel-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jroute-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jcrypto-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jweb-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using /var/tmp/config.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: warning: schema: init: 'logical-systems-vlans' contains-node 'juniper-config
  vlans': not found
```

```
mgd: commit complete  
Validation succeeded
```

request system storage cleanup

List of Syntax	Syntax on page 362 Syntax (EX Series Switches) on page 362 Syntax (MX Series Router) on page 362 Syntax (QFX Series) on page 362 Syntax (SRX Series) on page 362
Syntax	request system storage cleanup <dry-run>
Syntax (EX Series Switches)	<pre>request system storage cleanup <all-members> <dry-run> <local> <member member-id> <satellite [slot-id slot-id device-alias alias-name]></pre>
Syntax (MX Series Router)	<pre>request system storage cleanup <all-members> <dry-run> <local> <member member-id> <satellite [slot-id slot-id device-alias alias-name]></pre>
Syntax (QFX Series)	<pre>request system storage cleanup <component (serial number UUID all)> <director-group name> <dry-run> <infrastructure name> <interconnect-device name> <name-tag name-tag> <node-group name> <prune> <qfabric (component name) dry-run name-tag repository> <repository (core log)></pre>
Syntax (SRX Series)	<pre>request system storage cleanup <dry-run></pre>
Release Information	<p>Command introduced in Junos OS Release 7.4.</p> <p>dry-run option introduced in Junos OS Release 7.6.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 9.2 for SRX Series.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>satellite option introduced in Junos OS Release 14.2R3.</p>
Description	Free storage space on the router or switch by rotating log files and proposing a list of files for deletion. User input is required for file deletion. On a QFabric system, you can delete debug files located on individual devices or on the entire QFabric system.

Options **all-members**—(EX4200 switches and MX Series routers only) (Optional) Delete files on the Virtual Chassis master Routing Engine only.



NOTE: To delete files on the other members of the Virtual Chassis configuration, log in to each backup Routing Engine and delete the files using the **request system storage cleanup local** command.

component (*UUID | serial number | all*)—(QFabric systems only) (Optional) Delete files located on individual QFabric system devices or on the entire QFabric system.

director-group *name*—(QFabric systems only) (Optional) Delete files on the Director group.

dry-run—(Optional) List files proposed for deletion (without deleting them).

infrastructure *name*—(QFabric systems only) (Optional) Delete files on the fabric control Routing Engine and fabric manager Routing Engine.

interconnect-device *name*—(QFabric systems only) (Optional) Delete files on the Interconnect device.

local—(EX4200 switches and MX Series routers only) (Optional) Delete files on the local Virtual Chassis member.

member *member-id*—(EX4200 switches and MX Series routers only) (Optional) Delete files 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.

name-tag *name-tag*—(QFabric systems only) (Optional) Delete debug files that match a specific regular expression.

node-group *name*—(QFabric systems only) (Optional) Delete files on the Node group.

prune—(QFabric systems only) (Optional) Delete debug files located in either the core or log debug repositories of a QFabric system device.

qfabric component *name*—(QFabric systems only) (Optional) Delete debug files located in the debug repositories of a QFabric system device.

repository (*core | log*)—(QFabric systems only) (Optional) Specify the repository on the QFabric system device for which you want to delete debug files.

satellite [*slot-id slot-id | device-alias alias-name*]—(Junos Fusion only) (Optional) Specify the satellite device in the Junos Fusion by FPC ID or device alias name for which you want to delete debug files.

Additional Information If logging is configured and being used, the **dry-run** option rotates the log files. In that case, the output displays the message “Currently rotating log files, please wait.” If no logging is currently under way, the output displays only a list of files to delete.

Required Privilege Level maintenance

List of Sample Output [request system storage cleanup dry-run on page 365](#)
[request system storage cleanup on page 365](#)
[request system storage cleanup director-group \(QFabric Systems\) on page 365](#)
[request system storage cleanup infrastructure device-name \(QFabric Systems\) on page 367](#)
[request system storage cleanup interconnect-device device-name \(QFabric Systems\) on page 368](#)
[request system storage cleanup node-group group-name \(QFabric Systems\) on page 369](#)
[request system storage cleanup qfabric component device-name \(QFabric Systems\) on page 370](#)
[request system storage cleanup qfabric component device-name repository core \(QFabric Systems\) on page 370](#)
[request system storage cleanup qfabric component all \(QFabric Systems\) on page 371](#)

Output Fields [Table 45 on page 364](#) describes the output fields for the **request system storage cleanup** command. Output fields are listed in the approximate order in which they appear.

Table 45: request system storage cleanup Output Fields

Field Name	Field Description
List of files to delete:	Shows list of files available for deletion.
Size	Size of the core-dump file.
Date	Last core-dump file modification date and time.
Name	Name of the core-dump file.
Directory to delete:	Shows list of directories available for deletion.
Repository scope:	Repository where core-dump files and log files are stored. The core-dump files are located in the core repository, and the log files are located in the log repository. The default Repository scope is shared since both the core and log repositories are shared by all of the QFabric system devices.
Repository head:	Name of the top-level repository location.
Repository name:	Name of the repository: core or log .
Creating list of debug artifacts to be removed under:	Shows location of files available for deletion.
List of debug artifacts to be removed under:	Shows list of files available for deletion.

Sample Output

request system storage cleanup dry-run

```
user@host> request system storage cleanup dry-run
Currently rotating log files, please wait.
This operation can take up to a minute.
```

List of files to delete:

	Size	Date	Name
	11.4K	Mar 8 15:00	/var/log/messages.1.gz
	7245B	Feb 5 15:00	/var/log/messages.3.gz
	11.8K	Feb 22 13:00	/var/log/messages.2.gz
	3926B	Mar 16 13:57	/var/log/messages.0.gz
	3962B	Feb 22 12:47	/var/log/sampled.1.gz
	4146B	Mar 8 12:20	/var/log/sampled.0.gz
	4708B	Dec 21 11:39	/var/log/sampled.2.gz
	7068B	Jan 16 18:00	/var/log/messages.4.gz
	13.7K	Dec 27 22:00	/var/log/messages.5.gz
	890B	Feb 22 17:22	/var/tmp/sampled.pkts
	65.8M	Oct 26 09:10	/var/sw/pkg/jinstall-7.4R1.7-export-signed.tgz
	63.1M	Oct 26 09:13	/var/sw/pkg/jbundle-7.4R1.7.tgz

request system storage cleanup

```
user@host> request system storage cleanup
Currently rotating log files, please wait.
This operation can take up to a minute.
```

List of files to delete:

	Size	Date	Name
	11.4K	Mar 8 15:00	/var/log/messages.1.gz
	7245B	Feb 5 15:00	/var/log/messages.3.gz
	11.8K	Feb 22 13:00	/var/log/messages.2.gz
	3926B	Mar 16 13:57	/var/log/messages.0.gz
	11.6K	Mar 8 15:00	/var/log/messages.5.gz
	7254B	Feb 5 15:00	/var/log/messages.6.gz
	12.9K	Feb 22 13:00	/var/log/messages.8.gz
	3726B	Mar 16 13:57	/var/log/messages.7.gz
	3962B	Feb 22 12:47	/var/log/sampled.1.gz
	4146B	Mar 8 12:20	/var/log/sampled.0.gz
	4708B	Dec 21 11:39	/var/log/sampled.2.gz
	7068B	Jan 16 18:00	/var/log/messages.4.gz
	13.7K	Dec 27 22:00	/var/log/messages.5.gz
	890B	Feb 22 17:22	/var/tmp/sampled.pkts
	65.8M	Oct 26 09:10	/var/sw/pkg/jinstall-7.4R1.7-export-signed.tgz
	63.1M	Oct 26 09:13	/var/sw/pkg/jbundle-7.4R1.7.tgz

Delete these files ? [yes,no] (yes)

request system storage cleanup director-group (QFabric Systems)

```
user@switch> request system storage cleanup director-group
List of files to delete:
```

	Size	Date	Name
	4.0K	2011-11-07 05:16:29	/tmp/2064.sfcauth
	4.0K	2011-11-07 05:07:34	/tmp/30804.sfcauth
	4.0K	2011-11-07 04:13:41	/tmp/26792.sfcauth

```

4.0K 2011-11-07 04:13:39 /tmp/26432.sfcauth
0 2011-11-07 07:45:40 /tmp/cluster_cleanup.log
1.3M 2011-11-07 07:39:11 /tmp/cn_monitor.20111107-052401.log
4.0K 2011-11-07 07:36:29 /tmp/clustat.28019.log
4.0K 2011-11-07 07:36:29 /tmp/clustat_x.28019.log
9.6M 2011-11-07 05:30:24 /tmp/sfc.2.log
4.0K 2011-11-07 05:28:11 /tmp/mgd-init.1320672491.log
248K 2011-11-07 05:19:24 /tmp/cn_monitor.20111107-045111.log
4.0K 2011-11-07 05:17:18 /tmp/clustat.3401.log
4.0K 2011-11-07 05:17:18 /tmp/clustat_x.3401.log
8.0K 2011-11-07 04:58:25 /tmp/mgd-init.1320670633.log
0 2011-11-07 04:54:01 /tmp/mysql_db_install_5.1.37.log
4.0K 2011-11-07 04:52:08 /tmp/cn_send.log
0 2011-11-07 04:52:00 /tmp/init_eth0.log
4.0K 2011-11-07 04:49:35 /tmp/install_interfaces.sh.log
4.0K 2011-11-07 04:48:15 /tmp/bootstrap.sh.log
160K 2011-11-07 04:47:43 /tmp/bootstrap_cleanup.log
38M 2011-11-07 04:42:42 /tmp/cn_monitor.20111104-110308.log
4.0K 2011-11-07 04:38:47 /tmp/clustat.30913.log
4.0K 2011-11-07 04:38:47 /tmp/clustat_x.30913.log
4.0K 2011-11-07 04:38:03 /tmp/dcf_upgrade.sh.remove.log
4.0K 2011-11-07 04:38:03 /tmp/peer_update.log
4.0K 2011-11-07 04:38:02 /tmp/dcf_upgrade.log
4.0K 2011-11-07 04:38:02 /tmp/perl_mark_upgrade.log
8.0K 2011-11-07 04:13:42 /tmp/install_dcf_rpm.log
4.0K 2011-11-07 04:13:06 /tmp/00_cleanup.sh.1320667986.log
0 2011-11-07 04:13:06 /tmp/ccif_patch_4410_4450.sh.1320667986.log
4.0K 2011-11-07 04:13:06 /tmp/dcf-tools.sh.1320667986.log
0 2011-11-07 04:13:06 /tmp/initial.sh.1320667986.log
0 2011-11-07 04:13:06 /tmp/inventory.sh.1320667986.log
4.0K 2011-11-07 04:13:06 /tmp/qf-db.sh.1320667986.log
4.0K 2011-11-07 04:13:06 /tmp/sfc.sh.1320667986.log
8.0K 2011-11-07 04:13:05 /tmp/jinstall-qfabric.log
8.0K 2011-11-04 11:10:24 /tmp/mgd-init.1320430192.log
4.0K 2011-11-04 11:07:03 /tmp/mysql_dcf_db_install.log
8.0K 2011-11-04 10:55:07 /tmp/ccif_patch_4410_4450.sh.1320429307.log
8.0K 2011-11-04 10:55:07 /tmp/initial.sh.1320429307.log
4.0K 2011-11-04 10:55:07 /tmp/inventory.sh.1320429307.log
8.0K 2011-11-04 10:55:07 /tmp/sfc.sh.1320429307.log
4.0K 2011-11-04 10:54:09 /tmp/ks-script-Ax0tz5.log
4.0K 2011-11-07 04:13:06 /tmp//sfc.sh.1320667986.log
8.0K 2011-11-04 10:55:07 /tmp//sfc.sh.1320429307.log

```

Directory to delete:

```
45M 2011-11-08 10:57:43 /tmp/sfc-captures
```

List of files to delete:

Size	Date	Name
4.0K	2011-11-08 05:47:47	/tmp/5713.sfcauth
4.0K	2011-11-08 05:14:32	/tmp/14494.sfcauth
4.0K	2011-11-08 05:11:47	/tmp/9978.sfcauth
4.0K	2011-11-08 05:09:37	/tmp/6128.sfcauth
4.0K	2011-11-08 05:04:28	/tmp/29703.sfcauth
4.0K	2011-11-07 11:59:10	/tmp/7811.sfcauth
4.0K	2011-11-07 11:36:08	/tmp/32415.sfcauth
4.0K	2011-11-07 11:30:30	/tmp/22406.sfcauth
4.0K	2011-11-07 11:24:37	/tmp/12131.sfcauth
4.0K	2011-11-07 10:48:42	/tmp/12687.sfcauth
4.0K	2011-11-07 09:27:20	/tmp/31082.sfcauth
4.0K	2011-11-07 07:33:58	/tmp/14633.sfcauth

```

4.0K 2011-11-07 05:08:25 /tmp/15447.sfcauth
4.0K 2011-11-07 04:12:29 /tmp/26874.sfcauth
4.0K 2011-11-07 04:12:27 /tmp/26713.sfcauth
4.0K 2011-11-07 03:49:17 /tmp/17691.sfcauth
4.0K 2011-11-05 01:32:23 /tmp/5716.sfcauth
4.0K 2011-11-07 08:00:17 /tmp/sfcsnmpd.log
4.0K 2011-11-07 07:57:50 /tmp/cluster_cleanup.log
824K 2011-11-07 07:38:37 /tmp/cn_monitor.20111107-053643.log
4.0K 2011-11-07 07:36:30 /tmp/clustat.18399.log
4.0K 2011-11-07 07:36:30 /tmp/clustat_x.18399.log
4.0K 2011-11-07 07:35:47 /tmp/command_lock.log
4.0K 2011-11-07 05:39:54 /tmp/mgd-init.1320673194.log
92K 2011-11-07 05:19:25 /tmp/cn_monitor.20111107-050412.log
4.0K 2011-11-07 05:17:20 /tmp/clustat.30115.log
4.0K 2011-11-07 05:17:20 /tmp/clustat_x.30115.log
8.0K 2011-11-07 05:08:07 /tmp/mgd-init.1320671241.log
4.0K 2011-11-07 05:04:57 /tmp/cn_send.log
0 2011-11-07 05:04:52 /tmp/init_eth0.log
4.0K 2011-11-07 05:02:38 /tmp/install_interfaces.sh.log
4.0K 2011-11-07 05:01:19 /tmp/bootstrap.sh.log
160K 2011-11-07 05:00:47 /tmp/bootstrap_cleanup.log
28M 2011-11-07 04:42:27 /tmp/cn_monitor.20111104-112954.log
4.0K 2011-11-07 04:38:49 /tmp/clustat.6780.log
4.0K 2011-11-07 04:38:49 /tmp/clustat_x.6780.log
4.0K 2011-11-07 04:38:05 /tmp/issue_event.log
4.0K 2011-11-07 04:38:05 /tmp/peer_upgrade_reboot.log
12K 2011-11-07 04:38:05 /tmp/primary_update.log
4.0K 2011-11-07 04:38:04 /tmp/dcf_upgrade.sh.remove.log
4.0K 2011-11-07 04:38:04 /tmp/peer_rexec_upgrade.log
4.0K 2011-11-07 04:13:42 /tmp/peer_install_dcf_rpm.log
4.0K 2011-11-07 04:11:57 /tmp/dcf-tools.sh.1320667917.log
0 2011-11-07 04:11:57 /tmp/initial.sh.1320667917.log
0 2011-11-07 04:11:57 /tmp/inventory.sh.1320667917.log
4.0K 2011-11-07 04:11:57 /tmp/qlf-db.sh.1320667917.log
4.0K 2011-11-07 04:11:57 /tmp/sfc.sh.1320667917.log
4.0K 2011-11-07 04:11:56 /tmp/00_cleanup.sh.1320667916.log
0 2011-11-07 04:11:56 /tmp/ccif_patch_4410_4450.sh.1320667916.log
8.0K 2011-11-07 04:11:56 /tmp/jinstall-qlfabric.log
4.0K 2011-11-07 04:11:33 /tmp/dcf_upgrade.log
8.0K 2011-11-04 11:53:12 /tmp/mgd-init.1320432782.log
8.0K 2011-11-04 11:06:17 /tmp/ccif_patch_4410_4450.sh.1320429977.log
8.0K 2011-11-04 11:06:17 /tmp/initial.sh.1320429977.log
4.0K 2011-11-04 11:06:17 /tmp/inventory.sh.1320429977.log
8.0K 2011-11-04 11:06:17 /tmp/sfc.sh.1320429977.log
4.0K 2011-11-04 11:05:19 /tmp/ks-script_tnWeb.log
4.0K 2011-11-07 04:11:57 /tmp//sfc.sh.1320667917.log
8.0K 2011-11-04 11:06:17 /tmp//sfc.sh.1320429977.log

```

Directory to delete:

```
49M 2011-11-08 10:45:20 /tmp/sfc-captures
```

request system storage cleanup infrastructure device-name (QFabric Systems)

```
user@switch> request system storage cleanup infrastructure FC-0
re0:
```

List of files to delete:

Size	Date	Name
139B	Nov 8 19:03	/var/log/default-log-messages.0.gz

```

5602B Nov  8 19:03 /var/log/messages.0.gz
28.4K Nov  8 10:15 /var/log/messages.1.gz
35.2K Nov  7 13:45 /var/log/messages.2.gz
207B Nov  7 16:02 /var/log/wtmp.0.gz
27B Nov  7 12:14 /var/log/wtmp.1.gz
184.4M Nov  7 12:16
/var/sw/pkg/jinstall-dc-re-11.3I20111104_1216_dc-builder-domestic-signed.tgz
124.0K Nov  7 15:59 /var/tmp/gres-tp/env.dat
0B Nov  7 12:57 /var/tmp/gres-tp/lock
155B Nov  7 16:02 /var/tmp/krt_gencfg_filter.txt
0B Nov  7 12:35 /var/tmp/last_ccif_update
1217B Nov  7 12:15 /var/tmp/loader.conf.preinstall
184.4M Nov  6 07:11 /var/tmp/mchassis-install.tgz
10.8M Nov  7 12:16
/var/tmp/preinstall/bootstrap-install-11.3I20111104_1216_dc-builder.tar
57.4K Nov  7 12:16 /var/tmp/preinstall/configs-11.3I20111104_1216_dc-builder.tgz

259B Nov  7 12:16 /var/tmp/preinstall/install.conf
734.3K Nov  4 13:46
/var/tmp/preinstall/jboot-dc-re-11.3I20111104_1216_dc-builder.tgz
177.8M Nov  7 12:16
/var/tmp/preinstall/jbundle-dc-re-11.3I20111104_1216_dc-builder-domestic.tgz
124B Nov  7 12:15 /var/tmp/preinstall/metatags
1217B Nov  7 12:16 /var/tmp/preinstall_boot_loader.conf
0B Nov  7 16:02 /var/tmp/rtsdb/if-rtsdb

```

request system storage cleanup interconnect-device device-name (QFabric Systems)

```

user@switch> request system storage cleanup interconnect IC-WS001
re1:

```

```

-----
List of files to delete:

```

Size	Date	Name
11B	Nov 7 15:55	/var/jail/tmp/alarmd.ts
128B	Nov 8 19:06	/var/log/default-log-messages.0.gz
9965B	Nov 8 19:06	/var/log/messages.0.gz
15.8K	Nov 8 12:30	/var/log/messages.1.gz
15.8K	Nov 8 11:00	/var/log/messages.2.gz
15.7K	Nov 8 07:30	/var/log/messages.3.gz
15.8K	Nov 8 04:00	/var/log/messages.4.gz
15.7K	Nov 8 00:30	/var/log/messages.5.gz
18.7K	Nov 7 21:00	/var/log/messages.6.gz
17.6K	Nov 7 19:00	/var/log/messages.7.gz
58.3K	Nov 7 16:00	/var/log/messages.8.gz
20.3K	Nov 7 15:15	/var/log/messages.9.gz
90B	Nov 7 15:41	/var/log/wtmp.0.gz
57B	Nov 7 12:41	/var/log/wtmp.1.gz
124.0K	Nov 7 15:42	/var/tmp/gres-tp/env.dat
0B	Nov 7 12:40	/var/tmp/gres-tp/lock
0B	Nov 7 12:41	/var/tmp/if-rtsdb/env.lck
12.0K	Nov 7 15:41	/var/tmp/if-rtsdb/env.mem
132.0K	Nov 7 15:55	/var/tmp/if-rtsdb/shm_usr1.mem
2688.0K	Nov 7 15:41	/var/tmp/if-rtsdb/shm_usr2.mem
2048.0K	Nov 7 15:41	/var/tmp/if-rtsdb/trace.mem
730B	Nov 7 19:57	/var/tmp/juniper.conf+.gz
155B	Nov 7 15:53	/var/tmp/krt_gencfg_filter.txt
0B	Nov 7 15:41	/var/tmp/rtsdb/if-rtsdb

```

re0:

```

 List of files to delete:

	Size	Date	Name
	11B	Nov 7 15:55	/var/jail/tmp/alarmd.ts
	121B	Nov 8 19:06	/var/log/default-log-messages.0.gz
	16.7K	Nov 8 19:06	/var/log/messages.0.gz
	22.2K	Nov 8 17:45	/var/log/messages.1.gz
	18.4K	Nov 8 17:00	/var/log/messages.2.gz
	21.6K	Nov 8 16:00	/var/log/messages.3.gz
	17.9K	Nov 8 14:30	/var/log/messages.4.gz
	19.4K	Nov 8 13:30	/var/log/messages.5.gz
	18.2K	Nov 8 12:30	/var/log/messages.6.gz
	20.4K	Nov 8 11:30	/var/log/messages.7.gz
	21.4K	Nov 8 10:15	/var/log/messages.8.gz
	21.0K	Nov 8 09:00	/var/log/messages.9.gz
	19.9K	Nov 8 08:13	/var/log/snmp-traps.0.gz
	203B	Nov 8 15:36	/var/log/wtmp.0.gz
	57B	Nov 7 12:41	/var/log/wtmp.1.gz
	124.0K	Nov 7 15:42	/var/tmp/gres-tp/env.dat
	0B	Nov 7 12:40	/var/tmp/gres-tp/lock
	0B	Nov 7 12:41	/var/tmp/if-rtbdb/env.lck
	12.0K	Nov 7 15:41	/var/tmp/if-rtbdb/env.mem
	132.0K	Nov 7 15:55	/var/tmp/if-rtbdb/shm_usr1.mem
	2688.0K	Nov 7 15:41	/var/tmp/if-rtbdb/shm_usr2.mem
	2048.0K	Nov 7 15:41	/var/tmp/if-rtbdb/trace.mem
	727B	Nov 7 15:54	/var/tmp/juniper.conf+.gz
	155B	Nov 7 15:55	/var/tmp/krt_gencfg_filter.txt
	0B	Nov 7 15:41	/var/tmp/rtbdb/if-rtbdb

request system storage cleanup node-group group-name (QFabric Systems)

```
user@switch> request system storage cleanup node-group NW-NG-0
BBAK0372:
```

 List of files to delete:

	Size	Date	Name
	126B	Nov 8 19:07	/var/log/default-log-messages.0.gz
	179B	Nov 7 13:32	/var/log/install.0.gz
	22.9K	Nov 8 19:07	/var/log/messages.0.gz
	26.5K	Nov 8 17:30	/var/log/messages.1.gz
	20.5K	Nov 8 13:15	/var/log/messages.2.gz
	33.2K	Nov 7 17:45	/var/log/messages.3.gz
	35.5K	Nov 7 15:45	/var/log/messages.4.gz
	339B	Nov 8 17:10	/var/log/wtmp.0.gz
	58B	Nov 7 12:40	/var/log/wtmp.1.gz
	124.0K	Nov 8 17:08	/var/tmp/gres-tp/env.dat
	0B	Nov 7 12:39	/var/tmp/gres-tp/lock
	0B	Nov 7 12:59	/var/tmp/if-rtbdb/env.lck
	12.0K	Nov 8 17:09	/var/tmp/if-rtbdb/env.mem
	2688.0K	Nov 8 17:09	/var/tmp/if-rtbdb/shm_usr1.mem
	132.0K	Nov 8 17:09	/var/tmp/if-rtbdb/shm_usr2.mem
	2048.0K	Nov 8 17:09	/var/tmp/if-rtbdb/trace.mem
	1082B	Nov 8 17:09	/var/tmp/juniper.conf+.gz
	155B	Nov 7 17:39	/var/tmp/krt_gencfg_filter.txt
	0B	Nov 8 17:09	/var/tmp/rtbdb/if-rtbdb

EE3093:

 List of files to delete:

Size	Date	Name
11B	Nov 8 17:33	/var/jail/tmp/alarmd.ts
119B	Nov 8 19:08	/var/log/default-log-messages.0.gz
180B	Nov 7 17:41	/var/log/install.0.gz
178B	Nov 7 13:32	/var/log/install.1.gz
2739B	Nov 8 19:08	/var/log/messages.0.gz
29.8K	Nov 8 18:45	/var/log/messages.1.gz
31.8K	Nov 8 17:15	/var/log/messages.2.gz
20.6K	Nov 8 16:00	/var/log/messages.3.gz
15.4K	Nov 8 10:15	/var/log/messages.4.gz
15.4K	Nov 8 02:15	/var/log/messages.5.gz
25.5K	Nov 7 20:45	/var/log/messages.6.gz
48.0K	Nov 7 17:45	/var/log/messages.7.gz
32.8K	Nov 7 13:45	/var/log/messages.8.gz
684B	Nov 8 17:02	/var/log/wtmp.0.gz
58B	Nov 7 12:40	/var/log/wtmp.1.gz
124.0K	Nov 7 17:34	/var/tmp/gres-tp/env.dat
0B	Nov 7 12:40	/var/tmp/gres-tp/lock
0B	Nov 7 12:59	/var/tmp/if-rtbdb/env.lck
12.0K	Nov 7 17:39	/var/tmp/if-rtbdb/env.mem
2688.0K	Nov 7 17:39	/var/tmp/if-rtbdb/shm_usr1.mem
132.0K	Nov 7 17:40	/var/tmp/if-rtbdb/shm_usr2.mem
2048.0K	Nov 7 17:39	/var/tmp/if-rtbdb/trace.mem
155B	Nov 7 17:40	/var/tmp/krt_gencfg_filter.txt
0B	Nov 7 17:39	/var/tmp/rtbdb/if-rtbdb

request system storage cleanup qfabric component device-name (QFabric Systems)

```

user@switch> request system storage cleanup qfabric component A0001/YA0197
Repository type: regular
Repository head: /pbstorage
Creating list of debug artifacts to be removed under:
/pbstorage/rdumps/A0001/YA0197
Removing debug artifacts ... (press control C to abort)
Removing /pbstorage/rdumps/A0001/YA0197/cosd.core.0.0.05162011123308.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/cosd.core.1.0.05162011123614.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/cosd.core.2.0.05162011123920.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/livecore.05132011163930.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/tnetd.core.0.1057.05162011124500.gz ...
done
Removing /pbstorage/rdumps/A0001/YA0197/vmcore.05132011120528.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/vmcore.kz ... done
Creating list of debug artifacts to be removed under: /pbstorage/rlogs/A0001/YA0197
Removing debug artifacts ... (press control C to abort)
Removing /pbstorage/rlogs/A0001/YA0197/kdumpinfo.05132011120528 ... done
Removing /pbstorage/rlogs/A0001/YA0197/kernel.tarball.0.1039.05122011234415.tgz
... done
Removing /pbstorage/rlogs/A0001/YA0197/kernel.tarball.1.1039.05132011175544.tgz
... done
Removing /pbstorage/rlogs/A0001/YA0197/tnetd.tarball.0.1057.05162011175453.tgz
... done
  
```

request system storage cleanup qfabric component device-name repository core (QFabric Systems)

```

user@switch> request system storage cleanup qfabric component EE3093 repository core
Repository scope: shared
Repository head: /pbdata/export
  
```

```
Repository name: core
Creating list of debug artifacts to be removed under: /pbdata/export/rdumps/EE3093
NOTE: core repository under /pbdata/export/rdumps/EE3093 empty
```

request system storage cleanup qfabric component all (QFabric Systems)

```
user@switch> request system storage cleanup qfabric component all
Repository scope: shared
Repository head: /pbdata/export
Creating list of debug artifacts to be removed under: /pbdata/export/rdumps
NOTE: core repository under /pbdata/export/rdumps/all empty
Creating list of debug artifacts to be removed under: /pbdata/export/rlogs
List of debug artifacts to clean up ... (press control C to abort)
/pbdata/export/rlogs/73747cd8-0710-11e1-b6a4-00e081c5297e/install-11072011125819.log
/pbdata/export/rlogs/77116f18-0710-11e1-a2a0-00e081c5297e/install-11072011125819.log
/pbdata/export/rlogs/BBAK0372/install-11072011121538.log
/pbdata/export/rlogs/BBAK0394/install-11072011121532.log
/pbdata/export/rlogs/EE3093/install-11072011121536.log
/pbdata/export/rlogs/WS001/YN5999/install-11072011121644.log
/pbdata/export/rlogs/WS001/YW3803/install-11072011122429.log
/pbdata/export/rlogs/cd78871a-0710-11e1-878e-00e081c5297e/install-11072011125932.log
/pbdata/export/rlogs/d0afda1e-0710-11e1-a1d0-00e081c5297e/install-11072011125930.log
/pbdata/export/rlogs/d0afda1e-0710-11e1-a1d0-00e081c5297e/install-11072011133211.log
/pbdata/export/rlogs/d0afda1e-0710-11e1-a1d0-00e081c5297e/install-11072011155302.log
/pbdata/export/rlogs/d31ab7a6-0710-11e1-ad1b-00e081c5297e/install-11072011125931.log
/pbdata/export/rlogs/d4d0f254-0710-11e1-90c3-00e081c5297e/install-11072011125932.log
```

request system storage cleanup (SRX Series)

Syntax	<code>request system storage cleanup <dry-run></code>
Release Information	Command introduced in Junos OS Release 9.2 for SRX Series.
Description	Free storage space on the device by rotating log files and proposing a list of files for deletion. User input is required for file deletion.
Options	dry-run —(Optional) List files proposed for deletion (without deleting them).
Additional Information	If logging is configured and being used, the dry-run option rotates the log files. In that case, the output displays the message “Currently rotating log files, please wait.” If no logging is currently under way, the output displays only a list of files to delete.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • Cleaning Up Files with the CLI
List of Sample Output	request system storage cleanup dry-run on page 372 request system storage cleanup on page 374
Output Fields	Table 45 on page 364 describes the output fields for the request system storage cleanup command. Output fields are listed in the approximate order in which they appear.

Table 46: request system storage cleanup Output Fields

Field Name	Field Description
List of files to delete:	Shows list of files available for deletion.
Size	Size of the core-dump file.
Date	Last core-dump file modification date and time.
Name	Name of the core-dump file.

Sample Output

request system storage cleanup dry-run

```

user@host> request system storage cleanup dry-run
List of files to delete:

      Size Date      Name
  11B Jul 14 22:51 /var/jail/tmp/alarmd.ts
  84.3K Jul 20 22:09 /var/log/chassisd.0.gz
  83.0K Jul 20 04:35 /var/log/chassisd.1.gz
  84.0K Jul 19 10:52 /var/log/chassisd.2.gz
  90.4K Jul 18 17:16 /var/log/chassisd.3.gz

```

```

91.8K Jul 20 04:30 /var/log/hostlogs/auth.log.1.gz
93.1K Jul 17 05:45 /var/log/hostlogs/auth.log.2.gz
97.6K Jun 7 01:30 /var/log/hostlogs/auth.log.3.gz
92.0K Apr 25 15:15 /var/log/hostlogs/auth.log.4.gz
78.0K Jul 21 05:44 /var/log/hostlogs/daemon.log.1.gz
78.6K Jul 21 02:59 /var/log/hostlogs/daemon.log.2.gz
78.5K Jul 21 00:14 /var/log/hostlogs/daemon.log.3.gz
78.8K Jul 20 21:30 /var/log/hostlogs/daemon.log.4.gz
58.7K Jul 21 05:14 /var/log/hostlogs/debug.1.gz
58.5K Jul 21 00:59 /var/log/hostlogs/debug.2.gz
58.7K Jul 20 20:44 /var/log/hostlogs/debug.3.gz
58.7K Jul 20 16:29 /var/log/hostlogs/debug.4.gz
166.9K Jul 13 00:33 /var/log/hostlogs/kern.log.1.gz
166.5K Jun 1 02:32 /var/log/hostlogs/kern.log.2.gz
163.5K May 5 00:03 /var/log/hostlogs/kern.log.3.gz
152.3K Mar 2 23:23 /var/log/hostlogs/kern.log.4.gz
260.0K Apr 13 10:28 /var/log/hostlogs/lcmd.log.1.gz
257.3K Mar 7 00:38 /var/log/hostlogs/lcmd.log.2.gz
240.8K Feb 7 19:45 /var/log/hostlogs/lcmd.log.3.gz
241.1K Feb 7 14:00 /var/log/hostlogs/lcmd.log.4.gz
370.6K Jul 21 00:45 /var/log/hostlogs/syslog.1.gz
370.9K Jul 20 12:30 /var/log/hostlogs/syslog.2.gz
370.4K Jul 20 00:15 /var/log/hostlogs/syslog.3.gz
370.2K Jul 19 12:00 /var/log/hostlogs/syslog.4.gz
55.0K Jul 14 22:50 /var/log/hostlogs/vjunos0.log.1.gz
1467B Oct 28 2015 /var/log/install.0.gz
119.9K Jul 21 07:37 /var/log/messages.0.gz
147.4K May 27 01:30 /var/log/messages.1.gz
71.4K Apr 14 11:19 /var/log/messages.2.gz
90.7K Feb 28 14:15 /var/log/messages.3.gz
10.1K Jan 12 2016 /var/log/messages.4.gz
55.1K Jan 6 2016 /var/log/messages.5.gz
81.5K Dec 1 2015 /var/log/messages.6.gz
43.3K Oct 28 2015 /var/log/messages.7.gz
54.8K Oct 20 2015 /var/log/messages.8.gz
35.8K Oct 19 2015 /var/log/messages.9.gz
12.4K Jul 21 07:37 /var/log/security.0.gz
59.4K Jul 19 01:30 /var/log/security.1.gz
51.8K Apr 25 10:00 /var/log/security.2.gz
43.6K Apr 14 11:19 /var/log/security.3.gz
52.7K Apr 5 02:15 /var/log/security.4.gz
54.4K Mar 25 17:15 /var/log/security.5.gz
51.9K Mar 16 05:15 /var/log/security.6.gz
52.0K Mar 5 02:15 /var/log/security.7.gz
53.4K Feb 22 22:15 /var/log/security.8.gz
55.6K Feb 13 13:00 /var/log/security.9.gz
4063B Jul 14 22:51 /var/tmp/cleanup-pkgs.log
0B Jul 14 22:51 /var/tmp/eedebug_bin_file
50.9K Feb 8 20:33 /var/tmp/event_tags.php
34B Jul 14 22:51 /var/tmp/gksdchk.log
124.0K Apr 26 06:12 /var/tmp/gres-tp/env.dat
0B Oct 9 2015 /var/tmp/gres-tp/lock
4B Jul 14 22:52 /var/tmp/idp_license_info
46B Jul 14 22:51 /var/tmp/kmdchk.log
57B Jul 14 22:51 /var/tmp/krt_rpf_filter.txt
30B Jul 14 22:53 /var/tmp/policy_status
0B Jul 14 22:51 /var/tmp/rtsdb/if-rtsdb
349B Jul 14 22:51 /var/tmp/sd-upgrade/debug_log
0B Oct 9 2015 /var/tmp/spu_kmd_init
53B Feb 7 23:11 /var/tmp/vjunos-install.log
0B Jul 14 22:51 /var/tmp/vpn_tunnel_orig.id

```

request system storage cleanup

```
user@host> request system storage cleanup
```

```
List of files to delete:
```

	Size	Date	Name
	11B	Oct 28 23:40	/var/jail/tmp/alarmd.ts
	92.4K	Jan 11 17:12	/var/log/chassisd.0.gz
	92.4K	Jan 11 06:06	/var/log/chassisd.1.gz
	92.5K	Jan 10 19:00	/var/log/chassisd.2.gz
	92.5K	Jan 10 07:53	/var/log/chassisd.3.gz
	92.2K	Jan 10 15:00	/var/log/hostlogs/auth.log.1.gz
	92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.2.gz
	92.1K	Jan 4 17:30	/var/log/hostlogs/auth.log.3.gz
	92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.4.gz
	79.0K	Jan 12 01:59	/var/log/hostlogs/daemon.log.1.gz
	78.8K	Jan 11 23:15	/var/log/hostlogs/daemon.log.2.gz
	78.7K	Jan 11 20:30	/var/log/hostlogs/daemon.log.3.gz
	79.1K	Jan 11 17:44	/var/log/hostlogs/daemon.log.4.gz
	59.1K	Jan 11 21:59	/var/log/hostlogs/debug.1.gz
	59.2K	Jan 11 17:44	/var/log/hostlogs/debug.2.gz
	59.2K	Jan 11 13:29	/var/log/hostlogs/debug.3.gz
	59.3K	Jan 11 09:14	/var/log/hostlogs/debug.4.gz
	186.6K	Oct 20 16:31	/var/log/hostlogs/kern.log.1.gz
	238.3K	Jan 11 23:15	/var/log/hostlogs/lcmd.log.1.gz
	238.4K	Jan 11 17:30	/var/log/hostlogs/lcmd.log.2.gz
	238.6K	Jan 11 11:45	/var/log/hostlogs/lcmd.log.3.gz
	238.5K	Jan 11 06:00	/var/log/hostlogs/lcmd.log.4.gz
	372.5K	Jan 11 17:00	/var/log/hostlogs/syslog.1.gz
	372.5K	Jan 11 04:45	/var/log/hostlogs/syslog.2.gz
	371.9K	Jan 10 16:30	/var/log/hostlogs/syslog.3.gz
	372.7K	Jan 10 04:15	/var/log/hostlogs/syslog.4.gz
	10.1K	Jan 12 02:03	/var/log/messages.0.gz
	55.1K	Jan 6 21:25	/var/log/messages.1.gz
	81.5K	Dec 1 21:30	/var/log/messages.2.gz

```
Delete these files ? [yes,no] (no)
```

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 320](#)
- *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*
- [Reverting to the Rescue Configuration on page 186](#)
- [Reverting to the Default Factory Configuration by Using the request system zeroize Command on page 185](#)

List of Sample Output [request system zeroize on page 376](#)
[request system zeroize media on page 377](#)

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@host, 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@host:/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 `vnlrn' 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

```

```
(user@pool27.device.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@device.net:/volume/build/device/11.4/release/11.4R1.2/obj/
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
(user@device.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@device.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: HIDO 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 usb storage

Syntax	show chassis usb storage
Release Information	Command introduced in Junos OS Release 11.4 R2.
Description	Display the current status of any USB mass storage device and whether the USB ports are enabled or disabled.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Installing Junos OS on SRX Series Devices Using a USB Flash Drive on page 68
List of Sample Output	show chassis hardware detail on page 380 show chassis usb storage on page 380

Sample Output

show chassis hardware detail

```
user@host> show chassis hardware detail
Hardware inventory:
Item          Version  Part number  Serial number  Description
Chassis
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
  PIC 0
Power Supply 0
```

show chassis usb storage

```
user@host> show chassis usb storage
USB 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, and EX Series switches only) Display autoinstallation status information.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>ACX Series Autoinstallation Overview</i> • <i>Before You Begin Autoinstallation on an ACX Series Universal Access Router</i> • <i>Autoinstallation Configuration of ACX Series Universal Access Routers</i> • <i>USB Autoinstallation on ACX Series Routers</i> • <i>Verifying Autoinstallation on ACX Series Universal Access Routers</i> • <i>Autoinstalling a Configuration File from a Disk-on-Key USB Memory Stick onto an EX2200 or EX3300 Switch</i> • <i>autoinstallation</i>
List of Sample Output	show system autoinstallation status on page 382
Output Fields	Table 47 on page 381 describes the output fields for the show system autoinstallation status command. Output fields are listed in the approximate order in which they appear.

Table 47: show system autoinstallation status Output Fields

Field Name	Field Description
Autoinstallation status	Display autoinstallation status information: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Name—Name of the interface. • State—Interface state. • Address acquisition—Display IP address acquired and protocol used for acquisition upon startup. <ul style="list-style-type: none"> • 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 Junos OS Release 11.2.
Description	Perform checks and show status of all autorecovered items.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request system autorecovery state on page 290 • Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices on page 169
List of Sample Output	show system autorecovery state on page 383
Output Fields	Table 48 on page 383 lists the output fields for the show system autorecovery state command. Output fields are listed in the approximate order in which they appear.

Table 48: 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
s4

Saved
Saved

Passed
Passed

None
None

show system boot-messages

List of Syntax	Syntax on page 385 Syntax (EX Series Switches) on page 385 Syntax (TX Matrix Router) on page 385 Syntax (TX Matrix Plus Router) on page 385 Syntax (MX Series Router) on page 385 Syntax (QFX Series) on page 385
Syntax	show system boot-messages
Syntax (EX Series Switches)	show system boot-messages <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system boot-messages <all-chassis all-lcc lcc <i>number</i> scc>
Syntax (TX Matrix Plus Router)	show system boot-messages <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> >
Syntax (MX Series Router)	show system boot-messages <all-members> <local> <member <i>member-id</i> >
Syntax (QFX Series)	show system boot-messages infrastructure <i>name</i> interconnect-device <i>name</i> node-group <i>name</i>
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 <code>/var/run/dmesg.boot</code> .
Options	<p>none—Display all boot time messages.</p> <p>all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display boot time messages for all of the chassis.</p> <p>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.</p> <p>all-members—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on all members of the Virtual Chassis configuration.</p>

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 [show system boot-messages \(TX Matrix Router\) on page 387](#)
[show system boot-messages lcc \(TX Matrix Router\) on page 388](#)
[show system boot-messages \(TX Matrix Plus Router\) on page 389](#)
[show system boot-messages \(QFX3500 Switch\) on page 389](#)

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@device1.example.com:/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][FUNCO 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@device1.example.com:/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@device1.example.com:/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@device1.example.com:/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 system 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
    user@device1.example.com:/c/user/DEV_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
    user@device.net:/c/test/DEV_BRANCH/03/20100917.399988/
obj-xlr/bsd/sys/compile/JUNIPER-DCTOR
real memory = 3472883712 (3312MB)
avail memory = 1708171264 (1629MB)
cpuid: 0, bt1b_cpumap:0xffffffff8
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	<code>show system auto-snapshot</code>
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.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Understanding Resilient Dual-Root Partitions on Switches on page 95
List of Sample Output	show system auto-snapshot on page 393
Output Fields	Table 49 on page 392 describes the output fields for the <code>show system auto-snapshot</code> command. Output fields are listed in the approximate order in which they appear.

Table 49: show system auto-snapshot status Output Fields

Field Name	Field Description
Auto-snapshot configuration	Status of the configuration: <ul style="list-style-type: none"> • 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, <code>request system snapshot</code>, to take a snapshot of one partition and copy it onto the other.
Auto-snapshot state	Status of the automatic snapshot procedure: <ul style="list-style-type: none"> • 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	<code>show system download <download-id></code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
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	<ul style="list-style-type: none"> download-id—(Optional) The ID number of the download instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> request system download start on page 296 Understanding Download Manager for SRX Series Devices on page 51 Understanding Download Manager for EX Series Devices
List of Sample Output	show system download on page 394 show system download 1 on page 395
Output Fields	Table 50 on page 394 lists the output fields for the show system download command. Output fields are listed in the approximate order in which they appear.

Table 50: 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 URL from which the file was downloaded.

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 397 show system license installed on page 398 show system license keys on page 398 show system license usage on page 398 show system license (MX104 Routers) on page 398 show system license installed (MX104 Routers) on page 399 show system license keys (MX104 Routers) on page 399 show system license usage (MX104 Routers) on page 399 show system license (MX104 Routers) on page 399 show system license installed (MX104 Routers) on page 400 show system license keys (MX104 Routers) on page 400 show system license usage (MX104 Routers) on page 401 show system license (MX104 Routers) on page 401 show system license installed (MX104 Routers) on page 401 show system license keys (MX104 Routers) on page 402 show system license usage (MX104 Routers) on page 402 show system license (QFX Series) on page 402 show system license (QFX5110 Switch with Disaggregated Feature License) on page 402
Output Fields	Table 51 on page 397 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear.

Table 51: 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	<p>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.</p> <p>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.</p>
Licenses installed	<p>Information about the installed license key:</p> <ul style="list-style-type: none"> • 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. • Software Serial Number—Serial number of the disaggregated software feature license. License Management System (LMS) uses the software serial number, not the chassis ID, to generate a disaggregated feature license. • Customer ID—what is this exactly? • 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:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
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: XXXXXXXXXXXX
```

```
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: XXXXXXXXXXXX
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:

```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
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:

```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
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: XXXXXXXXXXXX
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: XXXXXXXXXXXX
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: XXXXXXXXXXXX
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: XXXXXXXXXXXX
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
```

Feature name	Licenses used	Licenses installed	Expiry 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:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
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 (QFX5110 Switch with Disaggregated Feature License)

```
user@switch> show system license
```

```
License usage:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
bgp	0	1	0	2017-07-05
00:00:00 UTC				
isis	0	1	0	2017-07-05
00:00:00 UTC				
vxlan	0	1	0	2017-07-05
00:00:00 UTC				
ovsdb	0	1	0	2017-07-05
00:00:00 UTC				
jbs1	0	1	0	2017-07-02
00:00:00 UTC				
upgrade1	0	1	0	2017-07-05
00:00:00 UTC				

```
Licenses installed:
```

```
License identifier: JUNOS797095
```

```
License version: 4
Software Serial Number: 91730A00223925
Customer ID: Juniper
Features:
  JUNOS-BASE-SERVICES-CLASS-1 - QFX Junos Base Services license for Class 1 HW
    date-based, 2016-07-01 00:00:00 UTC - 2017-07-02 00:00:00 UTC

License identifier: JUNOS797646
License version: 4
Software Serial Number: 91730A00224207
Customer ID: Juniper
Features:
  CLASS-1-JUNOS-BASE-ADVANCED-UPGRADE - Class 1 Junos Base to Advanced Services
  Upgrade
    date-based, 2016-07-04 00:00:00 UTC - 2017-07-05 00:00:00 UTC

{master:0}
```

show system license (View)

Syntax	show system license <installed keys status usage>
Release Information	Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.
Description	Display licenses and information about how licenses are used.
Options	<p>none—Display all license information.</p> <p>installed—(Optional) Display installed licenses only.</p> <p>keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.</p> <p>status—(Optional) Display license status for a specified logical system or for all logical systems.</p> <p>usage—(Optional) Display the state of licensed features.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying Junos OS License Installation on page 258
List of Sample Output	<p>show system license on page 405</p> <p>show system license installed on page 405</p> <p>show system license keys on page 406</p> <p>show system license usage on page 406</p> <p>show system license status logical-system all on page 406</p>
Output Fields	Table 52 on page 404 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear.

Table 52: 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 52: show system license Output Fields (*continued*)

Field Name	Field Description
Licenses installed	Information about the installed license key: <ul style="list-style-type: none"> • 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.
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:

```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine 01:00:00 IST	1	1	0	2012-03-30
wf_key_surfcontrol_cpa 01:00:00 IST	0	1	0	2012-03-30
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

Feature name                               Licenses  Licenses  Licenses  Expiry
          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	<ul style="list-style-type: none"> • <i>lockout-period</i> • clear system login lockout on page 289
List of Sample Output	show system login lockout on page 407
Output Fields	Table 53 on page 407 lists the output fields for the show system login lockout command. Output fields are listed in the approximate order in which they appear.

Table 53: 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 408](#)
[Syntax \(EX Series Switches\) on page 408](#)

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.
 Option **slice** deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

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 320](#)

List of Sample Output [show system snapshot \(Router\) on page 409](#)
[show system snapshot media external \(Switch\) on page 409](#)
[show system snapshot media internal \(Switch\) on page 410](#)

Output Fields [Table 54 on page 409](#) lists the output fields for the **show system snapshot** command. Output fields are listed in the approximate order in which they appear.

Table 54: 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/dals1a) (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/dals2a) (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 (Junos OS with Upgraded FreeBSD)

Syntax show system snapshot

Release Information Command introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers and EX9200 switches.
Command introduced in Junos OS Release 15.1X53-D30 for QFX5200 switches.

Description Display information about the non-recovery backup software, which is located in the **junos** file system on the hard disk drive or solid-state drive (SSD).



NOTE: To back up software, use the **request system snapshot** command.

Required Privilege Level view

Related Documentation

- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 327](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 314](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)

List of Sample Output [show system snapshot on page 411](#)

Output Fields When you enter this command, you are provided feedback on the status of your request. If there are no snapshots available, the command returns null output.

Sample Output

show system snapshot

```
user@host> show system snapshot
Snapshot snap.20141219.122106:
Location: /packages/sets/snap.20141219.122106
Creation date: Dec 19 12:21:06 2014
Junos version: 15.1-20141216_ib_15_1_psd.0
```

show system snapshot media

Syntax	show system snapshot media <i>media-type</i>
Release Information	Command introduced in Junos OS Release 10.2 .
Description	Display the snapshot information for both root partitions on SRX Series devices
Options	<ul style="list-style-type: none">• internal— Show snapshot information from internal media.• usb— Show snapshot information from device connected to USB port.• external— Show snapshot information from the external CompactFlash card.
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none">• Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166
List of Sample Output	show system snapshot media internal on page 412 show system snapshot media usb on page 412

Sample Output

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
```

show system storage partitions (EX Series Switches Only)

Syntax	show system storage partitions <all-members> <local> <member <i>member-id</i> >
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	<p>none—Display partition information.</p> <p>all-members—(Virtual Chassis systems only) (Optional) Display partition information for all members of the Virtual Chassis.</p> <p>local—(Virtual Chassis systems only) (Optional) Display partition information for the local Virtual Chassis member.</p> <p>member <i>member-id</i>—(Virtual Chassis systems only) (Optional) Display partition information for the specified member of the Virtual Chassis configuration.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 131
List of Sample Output	show system storage partitions on page 414
Output Fields	Table 55 on page 413 describes the output fields for the show system storage partitions command. Output fields are listed in the approximate order in which they appear.

Table 55: 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: <ul style="list-style-type: none"> • 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 Junos OS Release 10.2 .
Description	Display the partitioning scheme details on SRX Series devices.
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none"> • Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110
List of Sample Output	show system storage partitions (single root partitioning) on page 415 show system storage partitions (USB) on page 415

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 on page 419](#)

Index

Symbols

#, comments in configuration statements.....	xxiii
(), in syntax descriptions.....	xxiii
/altconfig directory	
altconfig file system.....	320
/altroot directory	
altroot file system.....	320
/config directory	
config file system.....	320
/config/juniper.conf file.....	15
/config/juniper.conf.1 file.....	15
/config/rescue.conf file.....	15
/etc/config/factory.conf file.....	15
64-bit	
Upgrade Routing Engine Junos OS.....	119
< >, in syntax descriptions.....	xxiii
[], in configuration statements.....	xxiii
{ }, in configuration statements.....	xxiii
(pipe), in syntax descriptions.....	xxiii

A

active	
configuration, logging	194
address	
command.....	199, 202
statement.....	199, 202
addresses	
configuring router.....	198, 202
default router.....	199, 203
hostname.....	198, 202
IP.....	199, 203
machine name.....	198, 202
altconfig, file system	197, 207, 208
altroot, file system	197, 207, 208
authentication	
root password.....	200, 204
auto-configuration.....	272, 273
auto-image-upgrade statement.....	275
auto-snapshot statement.....	276
auto-snapshot, displaying the status of.....	392

autoinstallation.....	84, 277
automatic configuration.....	91
automatic configuration process.....	83
default configuration file.....	83, 90
establishing.....	81
host-specific configuration file.....	83, 90
interfaces.....	82
IP address procurement process.....	83
overview.....	81
protocols for procuring an IP address.....	82
router.....	90
status.....	86
TFTP server.....	83, 90
verifying.....	86
autoinstallation statement	
for JNU satellites.....	278
autoinstallation, displaying the status of.....	381
automatic configuration See autoinstallation	

B

backing up current installation	
routers.....	55
backing up partitions.....	320
backup software, displaying information.....	408
backups	
copying to router.....	202, 206
file systems	197
software	207
BGP protocol	
logging information.....	195
boot devices	
alternative media.....	36
boot messages, displaying.....	385
boot sequence.....	15
M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series	
routing engines.....	35
SRX Series devices.....	37
bootp.....	279
braces, in configuration statements.....	xxiii
brackets	
angle, in syntax descriptions.....	xxiii
square, in configuration statements.....	xxiii
browser	
downloading software.....	49

C

category change software installation.....	41
--	----

chassis	
environment information, logging.....	191
hardware	
version, logging.....	190
chassis software process.....	17
chassisd process.....	17
checklist for	
reinstalling software	187
cleanup, storage space.....	362, 372
clear system login lockout command.....	289
command-line interface	
downloading software.....	49
commands for	
reinstalling software	187
comments, in configuration statements.....	xxiii
commit.....	280
config, file system.....	197, 207, 208
configuration	
autoinstallation of.....	81
downgrading software (CLI).....	156
downgrading software (J-Web).....	156
installation on multiple devices.....	81
upgrading (CLI).....	150
upgrading (J-Web).....	65
configuration files	
remote storage.....	16
sequence of selection.....	15
configuration, router	
active, logging	194
backup, copying	202, 206
configuration-servers.....	281
configure command	
backup configurations, copying.....	202, 206
names and addresses.....	198, 202
conventions	
text and syntax.....	xxii
creating a new router configuration.....	173
creating emergency boot device.....	165
curly braces, in configuration statements.....	xxiii
customer support.....	xxiv
contacting JTAC.....	xxiv
D	
daemons <i>See</i> processes, software	
default configuration file, for	
autoinstallation.....	83, 90
delete-after-commit statement	
for JNU satellites.....	282
deleting	
licenses (CLI).....	256
software packages.....	345
device	
autoinstallation.....	81
multiple, deploying <i>See</i> autoinstallation	
disk space, available	
managing.....	267
disk space, displaying	197
disk volume	
FreeBSD upgrade.....	24
documentation	
comments on.....	xxiii
domain name, configuring.....	199, 202
downgrading	
software, with J-Web.....	156
software, with the CLI	156
download URL.....	150
downloading	
configuration, with autoinstallation.....	83
software upgrades.....	150
downloading configuration, with	
autoinstallation.....	91
downloading Junos OS.....	48
dual-root partitioning.....	146
dual-root partitioning scheme.....	105
E	
emergency boot device	
booting from.....	36
creating.....	165
encrypted passwords.....	200, 204
encrypted-password option.....	200, 204
environment, logging information	191
erasing user data.....	375
Ethernet interface, configuring.....	199, 202
Ethernet ports	
autoinstallation on.....	82
F	
fans, showing environmental information.....	192
feature licenses <i>See</i> licenses	
file copy command.....	202, 206
file system	
/altconfig.....	197, 207, 208
/altroot	197, 207, 208
backing up.....	197
file systems	
partitions, backing up.....	320

- finalizing software installation.....63
 - FIPS See Junos-FIPS
 - flash drive, internal.....197
 - font conventions.....xxii
 - forwarding software process.....17
 - FreeBSD
 - validate.....359
 - FreeBSD upgrade
 - downgrading Junos OS.....209
 - Junos OS.....19
 - Junos OS disk volumes.....24
 - Junos OS package names.....22
 - Junos OS snapshots.....23
 - rebooting Junos OS.....314
 - upgrading Junos OS.....139
 - freeing up storage space.....362
 - fwdd process.....17
- H**
- halting a switching platform
 - with J-Web.....218
 - halting a switching platform immediately
 - with J-Web218
 - hard disk.....30
 - hardware
 - logging router chassis version190
 - hardware architecture
 - ACX Series, M Series, MX Series, T Series, and TX Matrix routers.....28
 - host-specific configuration file, for
 - autoinstallation.....83, 90
 - hostname, logging.....190
 - hostname.conf file, for autoinstallation.....83, 90
- I**
- ifd process.....17
 - Install Remote page
 - field summary.....65, 110, 153
 - installation
 - licenses (CLI).....255
 - memory requirements
 - M Series, MX Series, PTX Series, T Series, TX Matrix, and TX Matrix Plus routers.....29
 - on router with redundant Routing Engines.....58
 - on router with single Routing Engine.....57
 - software upgrades (CLI).....150
 - software upgrades, from a remote server.....65, 153
 - software upgrades, uploading.....65, 150
 - installation bundles.....13
 - installation media.....12
 - installation modules.....14
 - installation packages.....6
 - installation types.....41
 - installing software.....332, 333
 - interface software process.....17
 - interfaces
 - router, logging194
 - interfaces (autoinstallation).....283
 - IS-IS protocol
 - logging information194
 - ISSU See unified in-service software upgrade
- J**
- Junos OS
 - auto-snapshot status, displaying.....392
 - autoinstallation.....81
 - autoinstallation status, displaying.....381
 - backing up207
 - boot messages, displaying.....385
 - checklist for
 - reinstalling187
 - configuration files.....15
 - downgrading from upgraded FreeBSD.....209
 - downloading.....48
 - editions.....5
 - Canada and U.S.....5
 - Junos-FIPS.....5
 - worldwide.....5
 - FreeBSD upgraded.....19
 - information security.....11
 - installation
 - current configuration, confirming.....47
 - PIC combinations, verifying.....267
 - installation bundles.....13
 - installation media.....12
 - installation modules.....14
 - installation packages.....6
 - introduction.....3
 - logging version.....189
 - naming convention.....9
 - overview.....17
 - packages
 - digital signatures.....11
 - MD5 checksum.....11

naming conventions.....	11
SHA-1 checksum.....	11
Packet Forwarding Engine.....	17
processes.....	17
rebooting.....	307
rebooting with FreeBSD upgrade.....	314
reconfiguring.....	198
reinstalling.....	36, 197
using emergency boot devices.....	172
using removable media.....	172
release naming conventions.....	11
release numbers.....	11
Routing Engine.....	17
software installation types.....	41
storage media.....	30
device names.....	32, 34
Upgrade Routing Engine to 64-bit.....	119
upgrading.....	146
upgrading FreeBSD.....	139
version, displaying.....	48
Junos OS disk volumes	
FreeBSD upgraded.....	24
Junos OS package names	
FreeBSD upgraded.....	22
Junos OS snapshots	
FreeBSD upgraded.....	23
Junos OS versions See Junos OS editions	
JUNOS Software	
bundles, deleting.....	345
packages, deleting.....	345
rolling back.....	349
upgrade	
performing.....	332
validating candidate.....	355
Junos-FIPS.....	5
installation and configuration requirements.....	6
password requirements.....	6
K	
kernel	
downgrading from upgraded FreeBSD.....	209
FreeBSD upgrade.....	19
upgrading FreeBSD.....	139
L	
license infringement	
verifying license usage.....	259
verifying licenses installed.....	258
license keys	
components.....	223
licenses.....	223
adding.....	300
adding (CLI).....	255
deleting.....	301
deleting (CLI).....	256
displaying.....	396, 404
displaying (CLI).....	258
displaying usage.....	259
overview.....	221
saving.....	302
saving (CLI).....	257
verifying.....	258
limitations	
software downgrade cannot be undone.....	156
load command.....	343, 344
load merge command.....	202, 206
load replace command.....	202, 206
logical interfaces	
summary information.....	195
login lockout.....	289, 407
M	
management software process.....	17
managing	
reboots.....	218
software.....	146
manuals	
comments on.....	xxiii
MD5 (Message Digest 5) checksum.....	11
memory requirements	
M Series, MX Series, PTX Series, T Series, TX Matrix, and TX Matrix Plus routers.....	29
messages	
boot, displaying.....	385
mgd process.....	17
model, logging router	190
MPLS protocol, logging information.....	195
multiple devices	
deploying See autoinstallation	
Multiprotocol Label Switching See MPLS	
N	
name	
configuring domain	198, 202
configuring machine.....	198, 202
naming conventions, software.....	9

- network
 - connectivity, checking201, 206
 - ping command.....201, 206
- network.conf file, default for
 - autoinstallation.....83, 90
- O**
- operating system See Junos OS
- P**
- Packet Forwarding Engine.....17
- parentheses, in syntax descriptions.....xxiii
- partitions, backing up.....320
- password
 - root.....200, 204
 - root, setting200, 204
 - ssh public string.....201, 205
- passwords
 - for downloading software upgrades.....51, 150
- physical interfaces, summary information.....195
- PIC combinations
 - verifying during Junos OS installation.....267
- PIM protocol, logging information.....195
- ping command
 - network
 - connectivity, checking.....202, 206
- plain-text passwords
 - root password.....200, 204
- plain-text-password option.....200, 204
- Port Activation License Support
 - MX104.....226
- power supplies
 - environmental information.....192
- processes, software
 - chassis process.....17
 - forwarding process.....17
 - interface process.....17
 - management process.....17
 - routing protocol process.....17
- Protocol Independent Multicast See PIM
- R**
- reboot immediately
 - with J-Web.....218
- rebooting
 - with J-Web218
- rebooting router software
 - requesting a system reboot.....307
 - requesting a system reboot with FreeBSD
 - upgrade.....314
- reconfiguring Junos OS198
- recovery software installation.....42
 - procedures.....172
- registration form, for software upgrades.....147
- reinstall Junos OS
 - checklist.....187
 - comparing configurations.....206, 207
 - steps197
- reinstalling Junos OS.....172
- release names.....11
- remote server, upgrading from.....65, 153
- removable media
 - booting from.....36
 - reinstalling Junos OS, using.....172
- removing
 - software packages.....345
- request security idp security-package download
 - command.....305
- request system autorecovery state
 - command.....290
- request system download abort command.....292
- request system download clear command.....293
- request system download pause command.....294
- request system download resume command.....295
- request system download start command.....296
- request system firmware upgrade command.....297
- request system halt.....298
- request system license add command.....255, 300
- request system license add terminal
 - command.....255
- request system license delete command.....256, 301
- request system license save command.....257, 302
- request system license update command.....303
- request system partition compact-flash
 - command.....304
- request system reboot (FreeBSD upgrade)
 - command.....314
- request system reboot command.....307
- request system snapshot.....42, 329
- request system snapshot
 - command.....55, 56, 197, 207, 208, 320
- request system snapshot command (upgraded
 - FreeBSD).....327
- request system snapshot media command.....55

request system snapshot slice alternate command.....	55
request system software abort in-service-upgrade command.....	331
request system software add	342
request system software add command.....	332
request system software delete command.....	345
request system software rollback.....	42, 354
request system software rollback command.....	349
request system software validate command.....	355
request system software validate command (upgraded FreeBSD).....	359
request system storage cleanup command.....	362, 372
request system zeroize command.....	375
rescue configuration file saving.....	183
Resource Reservation Protocol See RSVP	
restoring a saved router configuration.....	184
reverting to a previous configuration file (J-Web).....	156
reverting to earlier software.....	350
rollback requesting.....	349
rolling back a configuration file, to downgrade software (CLI).....	156
root file system, backing up.....	197
root password.....	200, 204
root-authentication statement usage guidelines.....	200, 204
router.conf file, for autoinstallation.....	83
routers active configuration, logging	194
boot sequence.....	15
M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series routing engines.....	35
chassis hardware version, logging	190
check network connectivity.....	201, 206
configuring name and address.....	198, 202
copying backup configuration	202, 206
environment, logging.....	191
interfaces, logging.....	194
model, logging	190
storage media.....	30
Routing Engine environment information.....	192
software component.....	17
Upgrade to 64-bit Junos OS.....	119
Routing Engines available disk space, managing.....	267
backup installing software.....	59
illustrations.....	29
master installing software.....	61
storage media ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS routers.....	32
routing protocol software process.....	17
rpd process.....	17
RSVP protocol, logging information.....	195
S	
saving licenses (CLI).....	257
saving rescue configuration file.....	183
scheduling a reboot with J-Web.....	218
serial ports autoinstallation on.....	82
set interfaces address command	199, 202
set system backup-router command.....	199, 203
set system domain-name command.....	199, 202
set system host-name command.....	198, 202
set system name-server command.....	199, 203
set system root-authentication command.....	201, 205
set system root-authentication encrypted-password command.....	201, 205
setting root password.....	200, 204
SHA-1 (Secure Hash Algorithm) checksum.....	11
show bgp summary command.....	195, 206, 207
show chassis environment command.....	191, 206, 207
show chassis hardware command	190, 206, 207
show chassis routing-engine.....	29
show chassis routing-engine bios.....	69
show chassis usb storage command.....	380
show configuration command log active.....	194, 206, 207
show interface terse command.....	194, 206, 207
show isis adjacency brief command.....	195, 206, 207
show ospf neighbor brief command.....	195, 206, 207

- show route command.....202, 206
 - show system auto-snapshot status
 - command.....392
 - show system autoinstallation status
 - command.....86, 381
 - show system autorecovery state command.....383
 - show system boot-messages
 - command.....192, 206, 207, 385
 - show system download command.....394
 - show system license command.....258, 396, 404
 - explanation.....258
 - show system license usage command.....259
 - explanation.....259
 - show system login lockout command.....407
 - show system snapshot command.....408
 - show system snapshot command (FreeBSD upgrade).....411
 - show system snapshot media.....169, 412
 - show system storage.....34
 - show system storage command.....196, 206, 207
 - show system storage partitions.....415
 - show version.....48
 - show version command.....48, 189
 - compare information206, 207
 - reinstalling software.....189
 - snapshots
 - FreeBSD upgrade.....23
 - software.....17
 - halting immediately (J-Web)218
 - See also Junos OS
 - software categories
 - on M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers.....42
 - software installation
 - category change installation
 - description.....41
 - recovery installation
 - description.....42
 - standard installation
 - description.....41
 - software installation packages
 - Junos OS for SRX devices, domestic
 - description.....43
 - Junos OS for SRX devices, export
 - description.....43
 - Junos-FIPS
 - description.....42
 - standard Junos OS, domestic
 - description.....42
 - standard Junos OS, export
 - description.....42
 - software package names
 - FreeBSD upgrade.....22
 - software packages
 - upgrading individual.....116
 - software, Junos
 - backing up207
 - checklist for reinstalling.....187
 - logging hardware version.....190
 - logging software version189
 - packages
 - logging189
 - reconfiguring.....198
 - reinstalling.....197
 - SRX series device
 - bring components online/offline.....213
 - halting.....213
 - rebooting.....213
 - SRX series devices
 - software upgrades.....146
 - SRX Series Services Gateway.....166 See storage
- m e d i a
- auto bios upgrade methods.....155
 - configuring boot devices.....166
 - dual-root partitioning.....105
 - Install Remote page
 - field summary.....166
 - installing software
 - with CLI.....110
 - with J-Web.....110
 - Junos OS Release 10.0
 - upgrading without dual-root.....146
 - show system storage partitions.....113
 - snapshots.....166
 - software upgrade methods.....146
 - See also boot devices
 - SSH key files.....200, 204
 - standard software installation.....41
 - startup messages, displaying.....385
 - status
 - autoinstallation.....86

storage media.....	30	Upload package page	
device names		field summary.....	66
ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS		URLs	
routers.....	32	software downloads.....	150
M Series, MX Series, T Series, TX Series, and TX Matrix Plus routers.....	30	usb.....	286
storage space, freeing.....	362, 372	user data, erasing.....	375
support, technical See technical support		V	
switching platform		validate	
halting (J-Web).....	218	upgraded FreeBSD.....	359
rebooting (J-Web).....	218	validating software.....	355
syntax conventions.....	xxii	validating software compatibility.....	47
system		verification	
backup-router statement.....	199, 203	active licenses.....	258
boot-message, logging.....	192	autoinstallation.....	86
information, obtaining.....	206, 207	license usage.....	259
kernel messages, displaying.....	194	licenses	258
login lockout.....	289, 407		
storage, logging information.....	196		
system memory			
M Series, MX Series, T Series, TX series, and TX Matrix Plus routers.....	29		
system overview			
software.....	17		
T			
technical support			
contacting JTAC.....	xxiv		
temperature, environmental information.....	192		
TFTP, for autoinstallation.....	83, 90		
Trivial File Transfer Protocol (TFTP), for autoinstallation.....	83, 90		
U			
unified in-service software upgrade.....	122		
upgrade Junos OS			
comparing software.....	207		
upgraded FreeBSD			
validate.....	359		
upgrades			
downloading.....	150		
installing (CLI).....	150		
installing by uploading.....	65, 150		
installing from remote server.....	65, 153		
requirements.....	147		
upgrading or downgrading Junos OS.....	116		
upgrading software			
performing.....	332		