J-series Services Router Release Notes for JUNOS 8.3

Release 8.3R4
25 February 2008
Part Number: 530-018130-01
Revision 4

These release notes introduce the newest release of Juniper Networks J-series Services Routers and Release 8.3R4 of the JUNOS Internet software. They briefly describe J-series hardware features, identify known firmware and hardware problems, describe new J-Web features, and explain how to upgrade and downgrade the JUNOS Internet software and firmware on a Services Router.

For information about software features and problems, see the *JUNOS Internet Software Release Notes*. You can find the release notes on the Juniper Networks Technical Publications Web page, which is located at http://www.juniper.net/techpubs/.

Contents

J-series Services Router Features

This section describes the new J-series Services Routers features, available with the JUNOS 8.3R4 release. For more information, see the following manuals:

- *J4350 and J6350 Services Router Getting Started Guide*
- *J2300, J4300, and J6300 Services Router Getting Started Guide*
- *J-series Services Router Basic LAN and WAN Access Configuration Guide*
- *J-series Services Router Advanced WAN Access Configuration Guide*
- *J-series Services Router Administration Guide*

For more information about the JUNOS Internet software that runs on Services Routers, see the manuals listed in Table 6 on page 18.

Interfaces and Chassis

- **New high-density Gigabit Ethernet uPIMs**—Three new universal Physical Interface Modules (uPIMs) provide increased port density for Gigabit Ethernet connections. The uPIMs can be installed in either high-speed or regular slots on J4350 and J6350 Services Routers running JUNOS 8.3 or later. The new uPIMs are:
  - 8-port Gigabit Ethernet uPIMs with RJ-45 connectors
  - 16-port Gigabit Ethernet uPIMs with RJ-45 connectors (uses two slots)
  - 6-port Gigabit Ethernet uPIMs with small form-factor pluggable (SFP) connectors

CAUTION: You can install a maximum of three 8-port Gigabit Ethernet uPIMs in a single J4350 or J6350 chassis. If you install the maximum of three 8-port Gigabit Ethernet uPIMs, only one of the remaining slots can be occupied, and it cannot contain an ePIM, uPIM, or Avaya VoIP module.

For J-series Services Router PIM compatibility matrix and datasheets, go to http://www.juniper.net/products/jseries/.

- **ISDN PRI support on Channelized T1/E1/ISDN PRI PIMs**—Channelized T1/E1 PIMs are now called Dual-Port Channelized T1/E1/ISDN PRI PIMs and provide ISDN Primary Rate Interface (PRI) connectivity for dial-in and callback and for use as primary or backup network connections. You can configure up to 23 channelized T1 time slots or up to 30 channelized E1 time slots as an ISDN PRI group, with the 24th T1 time slot and the 16th E1 time slot operating as the D-channel to control the group of time slots as B-channels. T1 and E1 time slots unused by ISDN PRI can operate normally as DS0 interfaces. ISDN PRI B-channels run at 64 Kbps, but do not support the 56-Kbps line rate.

  ISDN PRI can operate in a Services Router chassis with ISDN BRI PIMs and supports ATT5ESS, ETSI (NET5), National ISDN (NI2), DMS100, and NTT switch types. The following ISDN features are supported:

- Bandwidth on demand with Multilink Point-to-Point Protocol (MLPPP)
- Dial-on-demand routing (DDR) backup
- Dial backup
- Authentication (CHAP and PAP)
- On-demand routing
- Dialer profiles and maps
- Dial-in
- Dialer callback

A new bchannel-allocation option enables you to allocate a free B-channel for dial-out calls. This setting directs the router to select the first free bchannel with highest number (default) or lowest when dialing out.

- **PAP support for PPP authentication**—Previously, PPP supported only CHAP authentication. PPP now supports the Password Authentication Protocol (PAP), a simple two-way handshake to establish identity. PAP is used after the link establishment phase (LCP up), during the authentication phase. JUNOS software can support PAP in one direction (egress or ingress), and CHAP in the other.

  To configure PAP support on the physical interface, include the pap statement with options at the [edit interfaces *interface-name* ppp-options] hierarchy level. To configure PAP support on the logical interface, include the pap statement with options at the [edit interfaces *interface-name* unit *logical-unit-number* ppp-options] hierarchy level. To view information about the PAP states, issue the show ppp summary and show ppp interfaces operational mode commands.

User Interface and Configuration

- **J-Web CLI terminal access**—You can now connect to the JUNOS CLI from the J-Web user interface by means of a Java applet running on the Web client. The applet provides SSH2 support to connect to the router. To access the CLI from J-Web, select **Diagnose > CLI Terminal**.
- **J-Web management enhancements**—You can now set the maximum number of simultaneous user sessions and a default session timeout for all users. To configure user sessions, include the session-limit and idle-timeout statements at the [edit system services web-management session] hierarchy level. You can also configure the maximum number of simultaneous subordinate processes in response to user requests, by including the active-child-process statement at the [edit system services web-management limits] hierarchy level. The show system users command now includes users who logged in or out through J-Web.
- **J-Web RPM timestamp support**—The J-Web Quick Configuration pages for real-time performance monitoring (RPM) now include a check box for enabling hardware timestamping for ICMP ping, ICMP ping timestamp, UDP ping, and UDP ping timestamp probes, to improve the measurement of latency and jitter.
- **Accounting files storage location setting**—The default location for accounting log files can now be set to the DRAM disk file system instead of the compact

flash. To configure this feature, include the nonpersistent statement at the [edit accounting-options file *filename*] hierarchy level. We recommend that you use the nonpersistent statement for all accounting files configured on your system. This setting minimizes the read/write traffic to the compact flash.

CAUTION: Because all files saved to DRAM are deleted when the system reboots, be sure to back up these files to ensure that they are not lost.

Network Management

- **RPM jitter enhancement for J-series Services Routers**—The way in which jitter for real-time performance monitoring (RPM) probes is calculated has been modified. Previously, jitter included delay on the other system and resulted in artificially high jitter numbers, which could imply that the network was experiencing more congestion than it actually was.
- **CoS scheduler transmit rate enhancement for J-series Services Routers**—The minimum size of the class-of-service (CoS) scheduler transmit rate is increased to 1/10000 of the interface speed (from the original limit of 1/1000 of the interface speed). The smaller increments provide finer control of transmit rate, which is especially useful for high-speed interfaces such as Fast Ethernet and Gigabit Ethernet interfaces on J4350 and J6350 routers.

  With the earlier minimum transmit rate you could only assign 1/1000th part of the interface speed. Therefore, if the speed of the interface was 1000 Mbps, the minimum transmit rate would be 1000 Mbps x 1/1000 = 1 Mbps. Now with the minimum transmit rate of 1/10000 for the same interface, you can set the transmit rate of a queue to be 1000 Mbps x 1/10000 = 100 Kbps.

Changes in Default Behavior and Syntax

- **Operational mode output change (J2320, J2350, J4350, and J6350 Services Routers)**—Previously, the show chassis fpc command output for selected J-series Services Routers showed just the slot into which a 2-slot-high PIM was physically inserted. Now the output of the show chassis fpc, show chassis fpc *slot*, and show chassis fpc *slot* detail commands also indicate the slot that is unusable.
- **Operational mode output change**—The show chassis hardware and show chassis environment commands now show the status of redundant power supply modules in the J6300 and J6350 Services Routers. In addition, the output of the show chassis alarms and show system alarms commands now includes power-module-related alarms, if present.
- **Setting a local loopback address**—If you configure a local loopback address using the loopback statement at the [edit interfaces *interface-name* gigether-options] hierarchy level, the transmit path stops working, causing the remote end to detect a down link.
- **New PIM abbreviation**—In show chassis hardware command output for J-series Services Routers, the 2x CT1E1 identifier for the Dual-Port Channelized T1/E1/ISDN

PRI PIM now appears as 2x CT1E1 / PRI to reflect the addition of ISDN PRI capability in the PIM.

- **Increase in number of dialer pools**—You can now configure up to 30 dialer pools on an ISDN PRI interface at the [edit interfaces *interface-name* dialer-options] hierarchy level. Previously the maximum was 16.
- **Removal of an unsupported encapsulation type**—Because flexible VLAN tagging is not supported on Fast Ethernet interfaces installed in J-series Services Routers, the flexible-vlan-tagging statement has been removed from the [edit interfaces fe-*pim*/0/*port*] hierarchy level in the CLI.
- **Removal of unsupported source address filtering statement**—The source-address-filter statement at the [edit interfaces *interface-name* gigether-options] hierarchy level has been deleted from the CLI, because J-series Gigabit Ethernet interfaces do not support MAC address filtering.
- **Change in options hierarchy for serial interfaces**—The control-leads statement at the [edit-interfaces se-*pim*/0/*port*] hierarchy level has been deprecated, and it is replaced by the dce-options statement. Serial interface functions and substatements remain unchanged. Although the control-leads statement still operates in existing configurations, use the dce-options statement for new configurations.
- **MTU configurable on multilink dialer interfaces**—You can now configure an MTU value on dialer interfaces with multilink encapsulation. To configure this setting, include the mtu statement at the [edit interfaces dl0 unit *logical-unit-number* family inet] hierarchy level.

Outstanding Issues

Platform and Infrastructure

- If you send a real-time performance monitoring (RPM) probe through an IPSec tunnel and the probe includes the hardware-timestamp statement at the [edit services rpm probe owner-name test test-name] hierarchy level, RPM ICMP ping type probes might not work. [PR/75927]
- On J4350 and J6350 Services Routers, if the MTU is set to more than 6 KB for a built-in Gigabit Ethernet port or a 1-port Gigabit Ethernet ePIM, packets might be discarded with a frame check sequence (FCS) error. [PR/82245]
- A user cannot log in to the J-Web client through RADIUS or TACACS+ authentication if the user profile already has authorization parameters specified on the server side. As a workaround, ensure that the user profile parameters are not specified or are set with empty values on the server. [PR/94445]

Interfaces and Chassis

- On channelized E1 interfaces, you might be able to configure clocking on ds-*pim*/0/*port*:*n* interfaces, where *n* is not unit 0. This is an invalid configuration and might cause a clocking selection problem on the other channels. [PR/24722]
- For ISDN dialer interfaces, when you configure the no-keepalives statement at the [edit interfaces dl0 unit *logical-unit-number*] hierarchy level and you issue the

show interfaces dl0 command, the Link flags field might still show keepalives. [PR/58520]

- If you disable a services interface by including the disable statement at the [edit interfaces sp-*pim*/0/*port*] hierarchy level and then delete the disable statement from the configuration, IPSec service is not reset correctly. As a workaround, either issue the deactivate services command followed by the activate services command, or issue the request chassis pic offline fpc-slot *pim-slot* pic-slot 0 command followed by the request chassis pic online fpc-slot *pim-slot* pic-slot 0 command. [PR/58522]
- When you take an ISDN interface offline, the LEDs on the ISDN PIM might not turn off. [PR/59536]
- On ISDN interfaces, if you configure the vrf-table-label statement at the [edit routing-instances *instance-name*] hierarchy level, packets might be dropped from the connection. [PR/59718]
- On ISDN dialer interfaces, if you configure the minimum-links statement at the [edit interfaces dl0 unit *logical-unit-number*] hierarchy level and then deactivate the BRI interface associated with the dialer interface, the output packets counter displayed in the output of the show interfaces dl0 command might continue to increment. [PR/59986]
- On ISDN dialer interfaces, when you configure the load-threshold 100 statement at the [edit interfaces dl0 unit *logical-unit-number* dialer-options] hierarchy level and the 56-Kbps bandwidth threshold is exceeded, the interface does not support additional network traffic and might not activate another BRI interface. [PR/60045]
- J4350 and J6350 Services Routers might not have the requisite data buffers needed to meet expected delay-bandwidth requirements. Lack of data buffers might degrade CoS performance with smaller-sized (500 bytes or less) packets. [PR/73054]
- On J4350 and J6350 Services Routers, when an Avaya TGM550 PIM is in reset state, the Services Router might not respond to show chassis commands for up to 5 seconds. [PR/78695]
- If you ping a nonexistent IPv6 address that belongs to the same subnet as an existing point-to-point link, the packet loops between the two point-to-point interfaces until the time-to-live timer expires. [PR/94954]
- On J-series Services Routers running JUNOS Release 8.3 or later, a Channelized T1/E1/ISDN PRI PIM running firmware version 2.3 or earlier might not initialize or might have clocking problems. After an upgrade to JUNOS 8.3 or later, verify the firmware version of any Channelized T1/E1/ISDN PRI PIM by issuing the show system firmware command. If the firmware version is not 2.4 or later, contact Juniper Networks customer support. [PR/102638]

Services Applications

- When you configure intrusion detection services (IDS) on J-series platforms, including the threshold statement at the [edit services ids rule *rule-name* term *term-name* then logging] hierarchy level has no effect. [PR/46577]

- If you configure an IPSec-over-GRE tunnel, there might be fragmentation issues. As a workaround, delete the clear-dont-fragment statement and the mtu statement on the GRE interface, and include the tunnel-mtu 9192 statement at the [edit services ipsec-vpn rule *rule-name* term *term-name* then] hierarchy level on both sides of the connection. [PR/74377]

Resolved Issues

The following issues have been resolved since JUNOS Release 8.3R3. The identifier following the description is the tracking number in our bug database.

- When you included the vrf-table-label statement at the [edit routing-instances routing-instance-name] hierarchy level, the incoming traffic was incorrectly considered to come from the internal label-switched interface (LSI) associated with the VRF instance that led to the router not accounting for the incoming traffic. [PR/53148: This issue has been resolved.]
- When you oversubscribed an E1 interface, latency on the high-priority queue was higher than expected. [PR/60595: This issue has been resolved.]
- In the J-Web configuration editor, when you selected System>Syslog >File >Messages >Explicit priority, the J-Web event viewer did not show the event ID. When you selected System>Syslog >Time format>Millisecond, the J-Web event viewer did not filter messages. [PR/70523: This issue has been resolved.]
- A J4350 or J6350 router running JUNOS Release 8.0 were not functioning properly when the Channelized T1/E1/ISDN PRI PIM or the Avaya TGM550, TIM510, TIM514, or TIM521 VoIP modules were installed on the router. [PR/74308: This issue has been resolved.]
- Dialer interface traffic statistics from the output of the show interfaces dl0 extensive command did not display input/output bytes in bps or input/output packets in pps. [PR/77922: This issue has been resolved.]

Errata

- J-Web Quick Configuration pages do not support IPv6 addressing and routing. [*J-series Services Router Basic LAN and WAN Access Configuration Guide*]
- Payload loopback functionality is not supported on ATM-over-SHDSL interfaces. [*J-series Services Router Basic LAN and WAN Access Configuration Guide*]
- JUNOS supports FRF.12 fragmentation header formats for both FRF.15 (MLFR) and FRF.16 (MFR).

  If you configure a permanent virtual circuit (PVC) between T1, E1, T3, or E3 interfaces in Juniper routing platform and another vendor and the other vendor does not have the same FRF.12 support or supports FRF.12 in a different way, the Juniper interface might discard a fragmented packet containing FRF.12 headers and count it as a "Policed Discard." As a workaround for this issue, configure multilink bundles on both peers and configure fragmentation thresholds

on the multilink bundle. [*J-series Services Router Basic LAN and WAN Access Configuration Guide*]

- For 4-port Fast Ethernet ePIMs on J4350 and J6350 Services Routers, if you apply a CoS scheduler map on outgoing (egress) traffic, the router does not divide the bandwidth appropriately among the CoS queues. As a workaround, configure enforced CoS shaping on the ports. [*J-series Services Router Advanced WAN Access Configuration Guide*]
- On J-series Services Routers, if you create a policy to match IPv4 traffic with a route filter and assign the traffic to a forwarding class, then apply the policy at the [edit class-of-service forwarding-policy class *policy-name*] hierarchy level, use of the classification-override statement at the [edit class-of-service forwarding-policy class *policy-name*] hierarchy level is not supported. [*J-series Services Router Advanced WAN Access Configuration Guide*]

J-series Chassis Power and Heat Capacities for PIM Combinations

Before you install a PIM, verify that the combination of PIMs installed in a chassis does not exceed the power and heat capacities for that model. The capacity of each chassis model and power and heat values required by each PIM can be represented in non-dimensional tokens.

CAUTION: Do not install a combination of PIMs in a single chassis that exceeds the power and heat capacities described in this section. Installing such a combination of PIMs in your router might cause equipment damage.

Add the token values for power and heat for each PIM or module that you want to install in a single chassis. The power tokens for a J4350 or J6450 chassis must not exceed 100. Likewise, the heat tokens must not exceed 100.

Table 1 on page 9 shows the power and heat dissipation tokens assigned to each J-series PIM or module.

Table 1: J-series PIM Power Consumption and Heat Dissipation

Name	Model Number	PIM Abbreviation in JUNOS CLI	Tokens	
			Power	Heat
16-Port Gigabit Ethernet uPIM	JXU-16GE-TX-S	16xGE uPIM	38	36
8-Port Gigabit Ethernet uPIM	JXU-8GE-TX-S	8xGE uPIM	21	27
6-Port Gigabit Ethernet uPIM	JXU-6GE-SFP-S	6xSFP uPIM	13	13
1-Port SFP Gigabit Ethernet ePIM	JXE-1GE-SFP-S	1xGE SFP	8	8
1-Port Copper Gigabit Ethernet ePIM	JXE-1GE-TX-S	1xGE Copper	6	7
4-Port Fast Ethernet ePIM	JXE-4FE-TX-S	4xFE ePIM	9	9
Dual-Port Fast Ethernet PIM	JX-2FE-TX-S	2xFE	6	6

Table 1: J-series PIM Power Consumption and Heat Dissipation *(continued)*

Name	Model Number	PIM Abbreviation in JUNOS CLI	Tokens	
			Power	Heat
ADSL 2/2 + Annex A PIM (1 port, for POTS)	JX-1ADSL-A-S	1x ADSL Annex A	16	16
ADSL 2/2 + Annex B PIM (1 port, for ISDN)	JX-1ADSL-B-S	1x ADSL Annex B	16	16
G.SHDSL PIM (2-port two-wire mode or 1-port four-wire mode)	JX-2SHDSL-S	2x SHDSL (ATM)	9	10
Dual-Port E1 PIM	JX-2E1–RJ48–S	2xE1	6	6
Dual-Port T1 PIM	JX-2T1–RJ48–S	2xT1	6	5
T3 PIM (also known as DS3)	JX-1DS3-S	1xT3	7	7
E3 PIM (1 port)	JX-1E3-S	1xE3	7	7
Dual-Port Channelized T1/E1/ISDN PRI PIM	JX-2CTE1-RJ45-S	2xCT1E1 / PRI	6	5
4-Port ISDN BRI S/T PIM	JX-4BRI-S-S	4x BRI S/T	4	4
4-Port ISDN BRI U PIM	JX-4BRI-U-S	4x BRI U	4	6
Dual-Port Serial PIM	JX-2Serial-S	2xSerial	5	6
TGM550 Telephony Gateway Module	Avaya	1x TGM550	14	19
TIM510 E1/T1 Telephony Interface Module	Avaya	1x DS1 TIM510	6	6
TIM514 Analog Telephony Interface Module	Avaya	4x FXS, 4xFXO TIM514	4	13
TIM521 BRI Telephony Interface Module	Avaya	4x BRI TIM521	3	3

Supported Third-Party Hardware

The following third-party hardware is supported for use with J-series Services Routers.

USB Modem

We recommend using a Multi-Tech MultiModem MT5634ZBA-USB-V92 USB modem with J-series Services Routers.

USB Storage Devices

The USB slots on J-series Services Routers accept a USB storage device or USB storage device adapter with a compact flash disk installed, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB device is installed and configured, it automatically acts as a secondary boot device if the primary compact flash disk fails on startup. Depending on the size of the USB storage device, you can also configure it to receive any core files generated during a router failure. The USB device must have a storage capacity of at least 256 MB.

Table 2 on page 11 lists USB storage devices supported for use with the J-series routers.

Table 2: Supported USB Storage Devices on the J-series Services Routers

Manufacturer	Storage Capacity	Part Number
SanDisk—Cruzer Mini 2.0	256 MB	SDCZ2-256-A10
SanDisk—ImageMate USB 2.0 Reader/Writer for CompactFlash Type I and II	N/A	SDDR-91-A15
SanDisk CompactFlash	512 MB	SDCFB-512-455
SanDisk CompactFlash	1 GB	SDCFB-1000–A10

Contact Juniper Networks customer support before using USB interfaces in a J-series Services Router.

J-series Compact Flash and Memory Requirements

Table 3 on page 11 lists the compact flash and DRAM requirements for all J-series Services Routers.

Table 3: J-series Compact Flash and DRAM Requirements

Model	Minimum Compact Flash Required	Minimum DRAM Required	Maximum DRAM Supported
J2300	256 MB	256 MB	1 GB
J4300	256 MB	256 MB	1 GB
J4350	256 MB	256 MB	2 GB
J6300	256 MB	256 MB	1 GB
J6350	256 MB	1 GB	2 GB

NOTE: If your J2300 Services Router contains a 128-MB compact flash, we recommend you upgrade it to at least 256 MB.

J-series Upgrade and Downgrade Instructions

This section contains the following topics:

NOTE: If the router is running a software version previous to JUNOS Release 7.2R3 or 7.3R2, you might need to upgrade to one of these interim software releases before you can upgrade to JUNOS Release 8.3R4.

Upgrade and Downgrade Overview

Typically, you upgrade the JUNOS software on a Services Router by downloading a set of images onto your router or onto another system on your local network, such as a PC. You then uncompress the package and install the uncompressed software using the CLI. Finally, you boot your system with this upgraded device.

A JUNOS software package is a collection of files that make up a software component. You can download software packages either for upgrading JUNOS software or for recovering a primary compact flash.

All JUNOS software is delivered in signed packages that contain digital signatures, Secure Hash Algorithm (SHA-1) checksums, and Message Digest 5 (MD5) checksums. For more information about JUNOS software packages, see the *JUNOS Software Installation and Upgrade Guide*.

Upgrade Software Packages

Download an upgrade software package, also known as an install package, to install new features and software fixes as they become available.

An upgrade software package name is in the following format: *package-name-m.nZx-distribution*.tgz.

- *package-name* is the name of the package—for example, junos-jseries.
- *m.n* is the software release, with *m* representing the major release number—for example, 8.0.
- *Z* indicates the type of software release. For example, R indicates released software, and B indicates beta-level software.
- *x* represents the version of the major software release—for example, 2.
- *distribution* indicates the area for which the software package is provided—domestic for the United States and Canada and export for worldwide distribution.

A sample J-series upgrade software package name is junos-jseries-8.0R2-domestic.tgz.

Recovery Software Packages

Download a recovery software package, also known as an install media package, to recover a primary compact flash device.

A recovery software package name is in the following format: *package-name-m.nZx*-export-cf*nnn*.gz.

- *package-name* is the name of the package—for example, junos-jseries.
- *m.n* is the software release, with *m* representing the major release number—for example, 8.0.
- *Z* indicates the type of software release. For example, R indicates released software, and B indicates beta-level software.
- *x* represents the version of the major software release—for example, 2.
- export indicates that the recovery software package is the exported worldwide software package version.
- cf*nnn* indicates the size of the target compact flash device in megabytes—for example, cf256.

A sample J-series recovery software package name is junos-jseries-8.0R2-export-cf256.gz.

Before You Begin

Before upgrading, be sure to back up the currently running and active file system and configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. To back up the file system, you must have a removable compact flash disk installed on a J4300 or J6300 Services Router, or a USB drive installed on any J-series Services Router. The backup device must have a storage capacity of at least 256 MB.

To back up the file system to the removable compact flash disk, issue the following command:

```
user@host> request system snapshot media removable-compact-flash
```

To back up the file system to the removable USB drive, issue the following command:

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

Before installing the software upgrade, issue the following command, which frees storage by rotating noncurrent log files in /var/log , deleting files in /var/tmp that have not been modified in two days, and deleting all crash files in /var/crash:

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

Before deleting the files, you can view the files to be deleted by issuing the following command:

```
user@host> request system storage cleanup dry-run
```

Downloading Software Upgrades from Juniper Networks

Follow these steps to download software upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks Web page. Depending on your location, select either **Canada and U.S. Version** or **Worldwide Version**:
   - https://www.juniper.net/support/csc/swdist-domestic/
   - https://www.juniper.net/support/csc/swdist-ww/
2. Log in to the Juniper Networks Web site 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 junos-j-series software package for your application. For information about JUNOS software packages, see “Upgrade and Downgrade Overview” on page 12.
4. Download the software to a local host or to an internal software distribution site.

NOTE: For downloads to J-series Services Routers with 256 MB of flash memory, see the *J-series Services Router Release Notes* for special instructions and ensure that you download the package to your router's /var/tmp/upgrade directory.

Installing Software Upgrades

Use either the J-Web interface or the CLI to install JUNOS software upgrades.

Installing Software Upgrades with the J-Web Interface

You can use the J-Web interface to install software upgrades from a remote server using FTP or HTTP, or by uploading the file to the router. This section contains the following topics:

Installing Software Upgrades from a Remote Server

You can use the J-Web interface to install software packages on the Internet Router that are retrieved with FTP or HTTP from the location specified.

To install software upgrades from a remote server:

1. Download the software package as described in "Downloading Software Upgrades from Juniper Networks" on page 14.
2. In the J-Web interface, select **Manage > Software > Install Package**.
3. On the Install Remote page, enter information into the fields described in Table 4 on page 15.
4. Click **Fetch and Install Package**. The software is activated after the router has rebooted.

Table 4: Install Remote Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name.	Type the full address of the software package location on the FTP or HTTP server—one of the following: ftp://*hostname/pathname/package-name* http://*hostname/pathname/package-name*
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	If this box is checked, the router is automatically rebooted when the upgrade is complete.	Check the box if you want the router to reboot automatically when the upgrade is complete.

Installing Software Upgrades by Uploading Files

You can use the J-Web interface to install software packages uploaded from your computer to the Internet Router.

To install software upgrades by uploading files:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 14.
2. In the J-Web interface, select **Manage > Software > Upload Package**.
3. On the Upload Package page, enter information into the fields described in Table 5 on page 16.
4. Click **Upload Package**. The software is activated after the router has rebooted.

Table 5: 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	If this box is checked the router is automatically rebooted when the upgrade is complete.	Select the check box if you want the router to reboot automatically when the upgrade is complete.

Installing Software Upgrades with the CLI

To install software upgrades on a router with the CLI:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 14.
2. If you are installing the software package from a local directory on the router, copy the JUNOS software package to the router. We recommend that you copy it to the /var/tmp directory.
3. Install the new package on the Services Router.

   user@host> **request system software add unlink no-copy** *source*

   Replace *source* with one of the following paths:

   - For a software package that is installed from a local directory on the router, use */pathname/package-name* (for example, /var/tmp/junos-jsr-8.5R2.1.tar.gz)
   - For software packages that are downloaded and installed from a remote location, use one of the following paths:
     - ftp://*hostname/pathname/package-name*

       or

     - http://*hostname/pathname/package-name*

   By default, the request system software add 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 router can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

The unlink option removes the package at the earliest opportunity so that the router has enough room to complete the installation.

(Optional) The no-copy option specifies that a software package is installed, but a copy of the package is not saved. Include this option if you do not have enough space on the compact flash to perform an upgrade that keeps a copy of the package on the router.

4. After the software package is installed, reboot the router:

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

When the reboot is complete, the router displays the login prompt.

Downgrade Instructions

This section contains the following topics:

NOTE: Juniper Networks supports direct software downgrades for a maximum of three releases. For example, if your routing platform is running JUNOS Release 7.6, you can typically downgrade without problems to Release 7.3. If you attempt to downgrade more than three releases and validation of your configuration fails, we recommend downgrading to an intermediate release first before downgrading to the desired release.

Downgrading the Software with the J-Web Interface

You can downgrade the software from the J-Web interface. For the changes to take effect, you must reboot the router.

To downgrade software:

1. In the J-Web interface, select **Manage > Software > Downgrade**. The image of the previous software version (if any) is displayed 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. When the downgrade process is complete, for the new software to take effect, select **Manage > Reboot** from the J-Web interface to reboot the router.

After you downgrade the software, the previous release is loaded, and you cannot reload the running version of software again. To downgrade to an earlier version of

software, follow the procedure for upgrading, using the JUNOS software image labeled with the appropriate release.

Downgrading the Software with the CLI

You can revert to the previous version of software using the request system software rollback command in the CLI. For the changes to take effect, you must reboot the router. To downgrade to an earlier version of software, follow the procedure for upgrading, using the JUNOS software image labeled with the appropriate release.

To downgrade software with the CLI:

1. Enter the request system software rollback command to return to the previous JUNOS software version:

   user@host> **request system software rollback**

   The previous software version is now ready to become active when you next reboot the router.

2. Reboot the router:

   user@host> **request system reboot**

The router is now running the previous version of the software.

Related Juniper Networks Documentation

Table 6 on page 18 lists and describes the publications for J-series Services Routers, the JUNOS CLI, the JUNOScript application programming interface (API), and the JUNOScope network management software.

Table 6: Juniper Networks Technical Documentation

Title	Description
J-series Guides	
Getting Started Guide	Provides an overview, basic instructions, and specifications for J-series Services Routers. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the Getting Started Guide for your router model.
J-series Services Router Basic LAN and WAN Access Configuration Guide	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.
J-series Services Router Advanced WAN Access Configuration Guide	Explains how to configure J-series Services Rout*JUNOS High Availability Configuration Guide*ers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPSec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.
J-series Services Router Administration Guide	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.

Table 6: Juniper Networks Technical Documentation *(continued)*

Title	Description
JUNOS Configuration Guides	
JUNOS Class of Service Configuration Guide	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
JUNOS CLI User Guide	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
JUNOS Feature Guide	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
JUNOS MPLS Applications Configuration Guide	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
JUNOS Multicast Protocols Configuration Guide	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
JUNOS Network Interfaces Configuration Guide	Provides an overview of the network interface functions of the JUNOS Internet software and describes how to configure the network interfaces on the routing platform.
JUNOS Network Management Configuration Guide	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
Secure Configuration Guide for Common Criteria and JUNOS-FIPS	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS Internet software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
JUNOS Software Installation and Upgrade Guide	Provides a description of JUNOS software components and packaging, and includes detailed information about how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
JUNOS Policy Framework Configuration Guide	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, forwarding options, and cflowd.
JUNOS Routing Protocols Configuration Guide	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
JUNOS Services Interfaces Configuration Guide	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
JUNOS System Basics Configuration Guide	Describes Juniper Networks routing platforms, and provides information about how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
JUNOS VPNs Configuration Guide	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
J-Web User Guide	

Table 6: Juniper Networks Technical Documentation *(continued)*

Title	Description
J-Web Interface User Guide	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS References	
JUNOS Hierarchy and RFC Reference	Describes the JUNOS *configuration mode* commands. Provides a hierarchy reference that displays each level of a configuration hierarchy and includes all possible configuration statements that can be used at that level. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
JUNOS System Basics and Services Command Reference	Describes the JUNOS software *operational mode* commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. This guide also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
JUNOS Interfaces Command Reference	Describes the JUNOS software *operational mode*commands you use to monitor and troubleshoot interfaces.
JUNOS Routing Protocols and Policies Command Reference	Describes the JUNOS software *operational mode* commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
JUNOS System Log Messages Reference	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
JUNOS API and Scripting Documentation	
JUNOScript API Guide	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routers.
JUNOS XML API Configuration Reference	Provides reference pages for the configuration tags in the JUNOScript API.
JUNOS XML API Operational Reference	Provides reference pages for the operational tags in the JUNOScript API.
JUNOS Configuration and Diagnostic Automation Guide	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
NETCONF API Guide	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
JUNOScope Software Documentation	
JUNOScope Software User Guide	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage router configuration files and monitor router operations.
Release Notes	
J-series Services Router Release Notes	Summarize new features, identify hardware problems, provide information omitted from the manual, and contain upgrade and downgrade instructions.

Table 6: Juniper Networks Technical Documentation *(continued)*

Title	Description
JUNOS Release Notes	Summarize new features for a particular software release, provide corrections and updates to published JUNOS and JUNOScript manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
JUNOScope Release Notes	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at http://www.juniper.net/techpubs/docbug/docbugreport.html. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for *Network Operations Guides [NOGs])*

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 JNASC support contract, or are covered under warranty, and need postsales 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/customers/support/downloads/710059.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: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Manager: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at 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 Manager 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, visit us at http://www.juniper.net/support/requesting-support.html.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the gzip utility, rename the file to include your company name, and copy it to ftp.juniper.net:pub/incoming. Then send the filename, along with software version information (the output of the show version command) and the configuration, to support@juniper.net. For documentation issues, fill out the bug report form located at http://www.juniper.net/techpubs/docbug/docbugreport.html.

Revision History

25 February 2008—Revision 4, JUNOS Release 8.3R4

17 October 2007—Revision 3, JUNOS Release 8.3R3

9 July 2007—Revision 2, JUNOS Release 8.3R2

18 April 2007—Revision 1, JUNOS Release 8.3R1