J-series Services Router Release Notes for JUNOS 8.2

Release 8.2R4
28 November 2007
Part Number: 530-017658-01
Revision R4

These release notes introduce the newest release of Juniper Networks J-series Services Routers and Release 8.2R4 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 8.2R4 release. For more information, see the following manuals:

- *J2300, J4300, and J6300 Services Router Getting Started Guide*
- *J4350 and J6350 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 5 on page 15.

Interfaces and Chassis

- **Integrated voice and data traffic on a single T1/E1 interface**—The drop-and-insert multiplexer is now integrated into channelized T1/E1 PIMs on Services Routers. On channelized T1/E1 interfaces partitioned into channels, you can insert time slots from one port directly into the other port on the same PIM, to replace time slots coming through the Routing Engine. To specify whether the channel sends and receives data from the Routing Engine (system) or the named interface, include the data-input system | interface *interface-name* statement at the [edit interfaces ds-*pim*/0/*port.:channel*] hierarchy level.

  To avoid slips, both ports must use the same clock source, either the router's internal clock or an external clock on one of the interfaces. If an external clock source is required, one interface must specify clocking external and the other must specify the same clock with clocking external interface *interface-name*.

NOTE: Before installing a channelized T1/E1 PIM on a Services Router, make sure the router is running JUNOS Release 8.1 or later. If you plan to downgrade the router to JUNOS 8.0 or earlier, remove the channelized T1/E1 PIM before you downgrade.

- **USB modems to remotely manage J-series Services Routers**—The Services Router now supports the use of USB modems for remote management. You can use Telnet or SSH to connect to the router from a remote location through two modems over a telephone network. One USB modem is connected to the USB port on the Services Router, and the second modem is connected to a remote management device such as a PC or laptop computer.

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

- **Larger delay buffers for channelized T1/E1 interfaces**—By default, interfaces other than channelized T1/E1 interfaces on Services Routers are limited to 100,000 microseconds of delay buffer. On channelized T1/E1 interfaces, the

default delay buffer is 500,000 microseconds for clear-channel interfaces, and 1,200,000 microseconds for *N*xDS0 interfaces. This feature allows you to configure larger delay buffers for the *N*xDS0 channelized T1/E1 interfaces to avoid congestion and packet dropping that occur when large bursts of traffic are received by slower interfaces. You can configure larger delay buffers for *N*xDS0 channelized T1/E1 interfaces only.

Services Applications

VoIP support on J4350 and J6350 Services Routers—J4350 and J6350 Services Routers support voice over IP (VoIP) routing with the Avaya IG550 Integrated Gateway. The Avaya IG550 Integrated Gateway consists of the following VoIP modules that are installed in the slots on J4350 and J6350 Services Routers:

- TGM550—Avaya Telephony Gateway Module (TGM) with two analog telephone ports, two analog trunk ports, and one serial port for console access
- TIM510—Avaya E1/T1 Telephony Interface Module (TIM) with one T1 or E1 trunk port
- TIM514—Avaya Analog TIM with four analog telephone ports and four analog trunk ports
- TIM521— Avaya BRI TIM with four RJ-45 ports for ISDN BRI trunk connections

The TGM550 is an H.248 media gateway that works with one or more TIMs to connect IP and legacy analog telephones and trunks over IP networks. The telephony services on the TGM550 are controlled by a Media Gateway Controller (MGC)—an Avaya media server running Avaya Communication Manager (CM) call processing software. The TGM550 is managed by an MGC located at headquarters or in a branch office. When the primary MGC is located at a remote location, the TGM550 uses standard local survivability (SLS) for partial MGC backup in the event that the connection to the primary MGC is lost.

NOTE: Before installing Avaya VoIP modules on a Services Router, make sure the router is running JUNOS Release 8.2. If you plan to downgrade the router to JUNOS 8.1 or earlier, remove the VoIP modules before you downgrade.

User Interface and Configuration

J-Web Quick Configuration support for static ARP addresses on Ethernet interfaces—Support for configuring static ARP addresses on Gigabit Ethernet and Fast Ethernet interfaces has been extended to the Quick Configuration pages on the J-Web interface. You can now configure static ARP addresses using the Interfaces Quick Configuration page.

Outstanding J-series Services Router Issues

The following problems currently exist in J-series Services Routers. The identifier following the description is the tracking number in the Juniper Networks bug database.

Platform and Infrastructure

- On J2320, J2350, J4350, and J6350 Services Routers, when you press the F10 key to save and exit from BIOS configuration mode, the operation might not work as expected. As a workaround, use the Save and Exit option from the Exit menu. This issue can be seen on the J4350 and J6350 routers with BIOS Version 080011 and on the J2320 and J2350 routers with BIOS Version 080012. [PR/237721]
- On J2320, J2350, J4350, and J6350 Services Routers, the Clear NVRAM option in the BIOS configuration mode does not work as expected. This issue can be seen on the J4350 and J6350 routers with BIOS Version 080011 and on the J2320 and J2350 routers with BIOS Version 080012. To help mitigate this issue, note any changes you make to the BIOS configuration so that you can revert to the default BIOS configuration as needed. [PR/237722]
- A J4350 or J6350 Services Router running JUNOS Release 8.0 will not function properly if the channelized T1/E1 PIM or the Avaya TGM550, TIM510, TIM514, or TIM521 VoIP modules are installed on the router. In addition, having these modules installed on a router running a JUNOS release that is too early can adversely affect the modules or the router configuration.

  To ensure that the router and the modules operate properly, take the following precautions:

  - Before you install a channelized T1/E1 PIM, upgrade the router to JUNOS Release 8.1 or later.
  - Before you install Avaya VoIP modules, upgrade the router to JUNOS Release 8.2.
  - Before you downgrade from JUNOS 8.2 or 8.1 to JUNOS 8.0, remove any channelized T1/E1 PIMs or Avaya VoIP modules installed on the router.

  [PR/74308]

Services Router User Interface and Configuration

The J-Web event viewer does not display the event ID for any event when you configure the system log file to include the message priority (facility name and severity level) in messages sent to a file:

- In the J-Web interface, by selecting **Configuration > System > Syslog > File >** *filename* **> Explicit priority**
- In the CLI, by including the explicit-priority statement at the [edit system syslog file *messages*] hierarchy level

You cannot filter events with the J-Web event viewer when you set the timestamp format for a system log file to milliseconds:

- In the J-Web interface, by selecting **Configuration > System > Syslog > Time format > Millisecond**
- In the CLI, by including the time-format millisecond statement at the [edit system syslog] hierarchy level

[PR/70523]

Interfaces and Chassis

- For ISDN dialer interfaces, when you include the no-keepalives statement at the [edit interfaces dl0 unit *logical-unit-number*] hierarchy level and you issue the show interfaces dl0 command, the output might display default keepalive settings. [PR/58520]
- If you disable a services interface by including the disable statement at the [edit interfaces sp-0/0/0] hierarchy level and then delete the disable statement from the configuration, the IPSec service might 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]
- If you take an ISDN interface offline, the LEDs on the ISDN PIM might not turn off. [PR/59536]
- For ISDN interfaces, if you include the vrf-table-label statement at the [edit interfaces routing-instances *routing-instance-name*] hierarchy level, packets might be dropped from the connection. [PR/59718]
- For ISDN dialer interfaces, if you include 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 command might continue to increment when the specified number of minimum links are not available. [PR/59986]
- For 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 threshold is exceeded, the interface does not support additional network traffic and might not activate another BRI interface. [PR/60045]
- If an ISDN dialer interface is configured as a dialer watch interface and is deactivated and configured as a backup interface, the dialer interface does not dial out when the primary interface becomes unavailable. As a workaround, disable the primary interface and commit the configuration, then enable the primary interface and commit the configuration. [PR/67355]
- If you send an RPM ICMP ping 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, the probe 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 an FCS error. [PR/82245]
- On serial interfaces transmitting either 64–byte or 128–byte packets, the effective bandwidth falls when the interface is highly oversubscribed. [PR/235753]

Class of Service

- If you oversubscribe an E1 interface, latency on the high-priority queue might be higher than expected. As a workaround, configure a shaping rate on the E1 interface that is equal to the line rate minus the E1 framing overhead. [PR/60595]
- 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]

Resolved Issues

The following issues have been resolved since JUNOS Release 8.2R3. The identifier following the description is the tracking number in the Juniper Networks bug database.

- If you include the vrf-table-label statement at the [edit routing-instances routing-instance-name] hierarchy level, the incoming traffic is considered to come from the internal label-switched interface (LSI) associated with the VRF instance. The traffic is not accounted for by the original incoming logical unit, because the original incoming logical interface is unknown and the LSI, being an internal interface, does not have accounting support. [PR/53148: This issue has been resolved.]
- When the chassis process (chassisd) restarted, an erroneous SNMP alarm for power supply failure was logged. [PR/100753: This issue has been resolved.]
- On J-series Services Routers configured with an IPSec tunnel, when you disabled the loopback interface, OSPF randomly chose a router ID and sent a routing update to the remote router using the IPSec tunnel endpoint, causing the packet to loop. Traffic forwarding stopped and a core file was generated. [PR/233271: This issue has been resolved.]
- On a J6350 Services Router with a Crypto Accelerator Module, when fragmented packets were processed the forwarding process generated a core file and stopped operating. [PR/251168: This issue has been resolved]
- When a large number of packets traversed a GRE-over-IPSec tunnel that has a J4350 Services Router with a Crypto Accelerator Module as one of its endpoints, the Services Router stopped forwarding traffic. [PR/101337: This issue has been resolved.]
- If you used a G.SHDSL interface in two-wire mode with an ADTRAN DSLAM, the 320-Kbps line rate did not work. [PR/62177: This issue has been resolved.]
- When a G.SHDSL interface initiates negotiations with an ADTRAN DSLAM, the G.SHDSL interface requires more than a minute to negotiate successfully. [PR/62462: This issue has been resolved.]
- On a J2300 Services Router with G.SHDSL interfaces installed, the line flaps at 320 Kbps with an ADTRAN DSLAM. [PR/64727; 64729: This issue has been resolved.]
- On a Dual-Port Channelized T1/E1 PIM, all links might not be available after the 24 individual time slots on one channelized T1 port are dropped and inserted into the 24 individual time slots on another channelized T1 interface on the same PIM. [PR/81976: This issue has been resolved]

Errata

- Payload loopback functionality is not supported on ATM-over-SHDSL interfaces. [*J-series Services Router Basic LAN and WAN Access Configuration Guide*]
- Information about FRF.12 specification for fragmenting Frame Relay frames on J-series Services Routers needs to be added to the J-series documentation. The standard for FRF.12 is defined in the specification FRF.12, *Frame Relay Fragmentation Implementation Agreement*. [*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*]
- The J-series documentation states that you can timestamp UDP ping and UDP ping timestamp RPM probes. However, the Services Router supports hardware timestamping of UDP ping and UDP ping timestamp RPM probes only if the destination port is UDP-ECHO. [*J-series Services Router Administration Guide*]

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 1 on page 9 lists USB storage devices supported for use with the J-series routers.

Table 1: 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	Model# SDDR-91-A15 20-90-0015
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 2 on page 9 lists the compact flash and DRAM requirements for all J-series Services Routers.

Table 2: 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	256 MB	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 8.2R4.

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 authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Using 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 10.
4. Download the software to a local host or to an internal software distribution site.

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 11.
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 3 on page 13.
4. Click **Fetch and Install Package**. The software is activated after the router has rebooted.

Table 3: 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 11.
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 4 on page 13.
4. Click **Upload Package**. The software is activated after the router has rebooted.

Table 4: 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 11.
2. Copy the 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 validate unlink reboot** *source*

   Replace *source* with one of the following paths:

   - For a software package that is installed from a local directory on the router—*/pathname/package-name*
   - For software packages that are downloaded and installed from a remote location:
     - ftp://*hostname/pathname/package-name*
     - http://*hostname/pathname/package-name*

   The validate option validates the software package against the current configuration as a prerequisite to adding the software package, to ensure that the router reboots successfully. This is the default behavior when you are adding a software package for a different release.

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

   Adding the reboot command reboots the router after the upgrade is validated and installed. Rebooting takes place only if the upgrade is successful.

   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. When you downgrade the software to a previous version, the software version that is saved in junos.old is the version of JUNOS that your router is downgraded to. For your changes to take effect, you must reboot the router.

To downgrade software:

1. Go to **Manage > Software > Downgrade**. The previous version (if any) is displayed on this page. For example, you can downgrade to the previously installed version of the router software, /cf/packages/junos-7.0120040930_1745-domestic.

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, click **Manage > Reboot** to reboot the router at your convenience.

Downgrading the Software with the CLI

You can revert to the previous set of software using the request system software rollback command in the CLI. Rollback fails if the junos-jseries software bundle cannot be found in /var/sw/pkg.

You can roll back only to the software release that was installed on the Services Router before the current release. After you issue the request system software rollback command, the old release is loaded and you cannot reload it again. Issuing the request system software rollback command again results in an error.

To downgrade to an earlier version of software, follow the procedure for upgrading, using the junos-jseries software bundle labeled for the appropriate release.

Related Juniper Networks Documentation

Table 5 on page 15 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 5: 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.

Table 5: Juniper Networks Technical Documentation *(continued)*

Title	Description
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.
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.

Table 5: Juniper Networks Technical Documentation *(continued)*

Title	Description
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	
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.

Table 5: Juniper Networks Technical Documentation *(continued)*

Title	Description
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.
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

Requesting Support

For technical support, open a support case with the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

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

28 November 2007—Revision R4, JUNOS Release 8.2R4

31 July 2007—Revision R3, JUNOS Release 8.2R3

20 March 2007—Revision R2, JUNOS Release 8.2R2

17 January 2007—Revision R1, JUNOS Release 8.2R1