

JUNOS Software with Enhanced Services 9.0 for J-series Services Router Release Notes

Release 9.0R4
November 2008
Part Number: 530-022949-01
Revision 4

These release notes accompany Release 9.0R4 of JUNOS software with enhanced services for J-series Services Routers. They briefly describe new software and hardware features and provide a summary of the current software limitations and known defects that exist in this release.



NOTE: J-series Services Routers are currently shipped with the JUNOS software. To install JUNOS software with enhanced services on your Services Router, see the *JUNOS Software with Enhanced Services Migration Guide*. The *J-series Services Router Quick Start* is shipped with the router. You can download the *JUNOS Software with Enhanced Services Quick Start* from the Juniper Web site at <http://www.juniper.net/techpubs/>.

You can also find these release notes on the Juniper Networks Technical Publications Web page located at <http://www.juniper.net/techpubs/>.

Contents

JUNOS Software with Enhanced Services Features	3
Hardware Support	3
Platform and Infrastructure	4
Interfaces and Chassis	4
Security Features	4
Routing and Interface Features	5
Management, Monitoring, and Configuration Features	6

WXC Integrated Service Module	7
Network Management	7
Changes in Default Behavior and Syntax	8
JUNOS Features Not Supported for Chassis Clusters	9
Outstanding Issues	9
Resolved Issues	12
Errata	12
Power and Heat Dissipation Requirements for J-series PIMs	12
Supported Third-Party Hardware	13
JUNOS Software with Enhanced Services Upgrade and Downgrade	
Instructions	13
Upgrade and Downgrade Overview	14
Upgrade Software Packages	15
Recovery Software Packages	15
Before You Begin	15
Downloading Software Upgrades from Juniper Networks	16
Installing Software Upgrades with the J-Web Interface	16
Installing Software Upgrades from a Remote Server	17
Installing Software Upgrades by Uploading Files	17
Installing Software Upgrades with the CLI	18
Installing Software Upgrades by Downloading Files	18
Installing Software Upgrades from a Remote Server	19
Downgrade Instructions	20
Downgrading the Software with the J-Web Interface	20
Downgrading the Software with the CLI	21
Special Instructions for J-series Routers with a 256-MB Compact Flash	21
Cleaning Up Files	22
Verifying Available Compact Flash Space	22
Removing the Swap Partition	23
List of Technical Publications	24
Documentation Feedback	31
Requesting Technical Support	31
Revision History	33

JUNOS Software with Enhanced Services Features

Release 9.0R4 of JUNOS software with enhanced services includes the following features. For more information, see the following manuals:

- *JUNOS Software with Enhanced Services Migration Guide*
- *JUNOS Software with Enhanced Services Getting Started Guide*
- *JUNOS Software with Enhanced Services Quick Start*
- *JUNOS Software with Enhanced Services Design and Implementation Guide*
- *JUNOS Software Interfaces and Routing Configuration Guide*
- *JUNOS Software Administration Guide*
- *JUNOS Software CLI Reference*
- *WXC Integrated Services Module Installation and Configuration Guide*

Hardware Support

You can install JUNOS software with enhanced services on the following J-series Services Routers. Most models support DS3 (T3), T1, Gigabit Ethernet, Fast Ethernet, E3, E1, serial, ATM-over-ADSL, ATM-over-SHDSL, Channelized T1/E1/ISDN PRI, and ISDN BRI interfaces.

- J2320 and J2350 (DS3 and E3 interfaces not supported)
- J4350
- J6350
- SSG320m and SSG350m (requires conversion kit)
- SSG520m and SSG550m (requires conversion kit)

For more information, see the *JUNOS Software with Enhanced Services Getting Started Guide*.

Platform and Infrastructure

- **Port mirroring and packet capture**—Port mirroring sends a copy of all network packets received on one switch port to a network monitoring connection on another switch port for analysis. Port mirroring is used for network applications such as intrusion detection systems that require monitoring of network traffic.

With packet capture, you can now capture packets with Multilink Point-to-Point Protocol (MLPP) and Multilink Frame Relay (MFR) encapsulation for analysis.

For information about packet capture, see the *JUNOS Software Administration Guide*.

Interfaces and Chassis

- **Support for chassis clustering**—You can now connect the chassis of two J-series Services Routers to provide stateful failover of JUNOS software with enhanced services processes and services. Interchassis clustering removes the single point of failure in the network by allowing Services Routers to be configured in a redundant cluster, with one router acting as the primary and the other as a backup. If the primary fails, the backup takes over traffic processing. Clustered routers, synchronize configuration, kernel, and Packet Forwarding Engine session states across the cluster to facilitate high availability of interfaces and services.

JUNOS software with enhanced services includes the following chassis cluster features:

- Resilient system architecture includes a single control plane for the entire cluster to manage multiple Packet Forwarding Engines.
- Configuration and dynamic runtime states are synchronized between the routers within a cluster.
- Graceful restart of the routing protocols enables the router to minimize traffic disruption during a failover.
- Physical interfaces are grouped and monitored to trigger failover to the backup Services Router if the failure parameters cross a configured threshold.

For more information, see the *JUNOS Software Security Configuration Guide*



NOTE: When configuring chassis clusters you are automatically in **configure private** mode. As a result, you must commit changes from the top of the hierarchy. For information about the **configure private** mode, see the *JUNOS CLI User Guide*.

Security Features

- **SCEP for IKE and IPSec**—JUNOS software with enhanced services now supports the Simple Certificate Enrollment Protocol (SCEP), an advanced public key infrastructure (PKI) feature for Internet Key Exchange (IKE) and IPSec authentication. Currently, PKI supports manual loading of both local end-entity

(EE) certificates and certificate authority (CA) certificates to authenticate entities for IKE. SCEP, however, allows the J-series Services Router to do the following:

- Verify the identity of the CA and load the CA certificate automatically.
- Obtain a certificate for its own identity.
- Enroll for multiple EE certificates from multiple CA servers.
- Re-enroll a certificate automatically before the current certificate expires.

For more information, see the *JUNOS Software Security Configuration Guide*.

Routing and Interface Features

- **MPLS support**—JUNOS software with enhanced services now supports Multiprotocol Label Switching (MPLS) to provide a framework for controlling traffic patterns across a network. The MPLS framework allows Services Routers to pass traffic through transit networks on paths that are independent of the individual routing protocols enabled throughout the network. The MPLS framework supports traffic engineering and the creation of virtual private networks (VPNs). Traffic is engineered (controlled) primarily by the use of signaling protocols to establish label-switched paths (LSPs). VPN support includes Layer 2 and Layer 3 VPNs and Layer 2 circuits.

For more information, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

- **Support for point-to-multipoint MPLS LSPs**—A point-to-multipoint MPLS label-switched path (LSP) is a Resource Reservation Protocol (RSVP)-signaled LSP with a single source and multiple destinations. By taking advantage of the MPLS packet replication capability of the network, point-to-multipoint LSPs avoid unnecessary packet replication at the ingress router. Packet replication takes place only when packets are forwarded to two or more different destinations requiring different network paths.

Point-to-multipoint LSPs allow you to

- Use MPLS for point-to-multipoint data distribution. This functionality is similar to that provided by IP multicast.
- Add and remove branch LSPs from a main point-to-multipoint LSP without disrupting traffic. The unaffected parts of the point-to-multipoint LSP continue to function normally.
- Configure a Service Router to be both a transit and an egress router for different branch LSPs of the same point-to-multipoint LSP.



NOTE: In JUNOS software with enhanced services, MPLS is disabled by default. You must explicitly configure your router to allow MPLS traffic to pass through. When you enable MPLS, all flow-based security features are deactivated and the router performs packet-based processing. For a list of packet-based services available on the router, see the *JUNOS Software Security Configuration Guide*. To enable MPLS on your router, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

- **Support for basic RPC ALG services**—Remote Procedure Call (RPC) is a protocol that allows an application running in one address space to access the resources of applications running on another address space as if the resources were local to the first address space. The RPC Application Layer Gateway (ALG) is responsible for RPC packet processing.

The RPC ALG in JUNOS software with enhanced services supports the following services and features:

- Sun Microsystems RPC Open Network Computing (ONC)
- Microsoft RPC Distributed Computing Environment (DCE)
- Dynamic port negotiation
- Ability to allow and deny specific RPC services
- Static NAT and source NAT (with no port translation)
- RPC applications in security policies

The RPC ALG is enabled by default. For more information, see the *JUNOS Software Security Configuration Guide*.

Management, Monitoring, and Configuration Features

- **J-Web Quick Configuration pages for chassis clusters**—The J-Web interface adds Quick Configuration pages for the new chassis cluster feature that provides redundant, high availability routing support. You can configure a redundancy group (cluster), the connecting redundant Ethernet interfaces, and flow forwarding for security.

For more information, see the *JUNOS Software Security Configuration Guide*.

- **J-Web Quick Configuration and Monitor pages for DNS**—The J-Web interface now provides Quick Configuration and Monitor pages for Domain Name System (DNS) proxy and dynamic DNS (DDNS). Quick Configuration pages allow you to enable DNS on configured interfaces, add interfaces, select name servers for the DNS proxy feature, and add and configure a DNS proxy cache. You can also add or edit dynamic DNS table entries. New Monitor pages provide a DNS proxy summary and allow you to monitor the DNS proxy cache and dynamic DNS table.

For more information, see the *JUNOS Software Administration Guide*.

- **J-Web Quick Configuration and Monitor pages for DHCP**—The J-Web interface now provides Quick Configuration and monitor pages for Dynamic Host Configuration Protocol (DHCP) server, client, and relay features. The Quick Configuration pages enable you to configure:
 - DHCP service global settings, DHCP pool address ranges, and static bindings
 - Interface-based DHCP clients
 - Forwarding of incoming BOOTP/DHCP relay requests

New Monitor pages enable you to monitor:

- Global scope and DHCP service statistics
- DHCP client bindings
- DHCP address conflicts
- DHCP clients
- DHCP relay statistics

For more information, see the *JUNOS Software Security Configuration Guide*.

WXC Integrated Service Module

- **WXC Integrated Services Module 200 for J-series routers**—The WXC Integrated Services Module (ISM 200) can be added to J2320, J2350, J4350, and J6350 Services Routers running JUNOS software with enhanced services. The module occupies two slots, and provides WAN traffic optimization and acceleration. For more information, see the *WXC Integrated Services Module Installation and Configuration Guide*.

Network Management

- **CoS queuing, scheduling, and traffic shaping on GRE and IP tunnels**—Generic routing encapsulation (GRE) and IP over IP (IP-IP) tunnels are used in services such as IPsec and Network Address Translation (NAT) to set up point-to-point virtual private networks (VPNs). Class-of-service (CoS) queuing enabled for outbound (egress) tunnel interfaces allows you to:
 - Configure tunnel-specific shaping rates by selecting CoS parameters for each tunnel, so that traffic to some sites gets better bandwidth than traffic to other sites.
 - Enhance user control over the traffic. Each tunnel can have different scheduler maps, queue depths, and so on.
 - Prioritize high-priority packets over low-priority packets. Each tunnel can be shaped, so that a tunnel with low-priority traffic cannot swamp other tunnels that carry high-priority traffic.

For more information, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

- **CoS improvements**—Class-of-service (CoS) operation on J-series Services Routers has been improved to reduce latency for high-priority packets and to protect control packets from delays on both outbound (egress) and inbound (ingress) traffic, especially on serial, ADSL, and SHDSL interfaces.
- **Hardware timestamp and MIB support for RPM jitter measurement**—Real-time performance monitoring (RPM) on J-series Services Routers running JUNOS software with enhanced services now includes the following features:
 - SNMP MIB support for additional timestamps to measure jitter for round-trip probes and probes in both the egress (source-to-destination) and ingress (destination-to-source) directions
 - SNMP MIB support for separate sets of statistics (minimum, maximum, average, peak to peak, standard deviation, and number of samples) for positive and negative measures of jitter for probes in the round-trip, ingress, and egress directions
 - SNMP MIB support for hardware timestamp probes

For more information, see the *JUNOS Software Administration Guide*.

Changes in Default Behavior and Syntax

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the JUNOS software with enhanced services documentation:

- **Firewall screens**—The default values for threshold limit for screen have been increased. [*JUNOS Software Security Configuration Guide*]
- **For Security**—J-series Services Routers do not support the authentication order `password radius` or `password ldap` in the `edit access profile profile-name authentication-order` command. Instead, use the `order radius password` or `ldap password`. [*JUNOS Software Security Configuration Guide*]
- **IPSec VPNs** —Previously, when you committed an IPSec VPN configuration, the J-series router needed to restart the IPSec process for the tunnel to come up. Now, when you commit an IPSec VPN configuration, the system restarts the IPSec process and does not require an IPSec process restart. [*JUNOS Software Interfaces and Routing Configuration Guide*]
- **No IPSec SAs in BGP**—JUNOS software with enhanced services does not support the use of IPSec security associations (SAs) in BGP protocol configuration. The `ipsec-sa` option is not available at the `edit protocols bgp` hierarchy level. [*JUNOS Software CLI Reference*]
- **Source and destination-based threshold limits for screens**—Previously, JUNOS software with enhanced services defined the source and destination-based threshold limits for security screens as low and did not allow you to increase them. Now you can increase the threshold as per traffic requirements. [*JUNOS Software Security Configuration Guide*]

JUNOS Features Not Supported for Chassis Clusters

For this release of JUNOS software with enhanced services, the following features are not supported when chassis clustering is enabled on the router:

- **Packet-based protocols.** All packet-based protocols, such as Multiprotocol Label Switching (MPLS), Connectionless Network Service (CLNS), and IP version 6 (IPv6)
- **Services interfaces functions.** Any function that depends on the configurable J-series services interfaces:
 - `ls-0/0/0`—Link services Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Compressed Real-Time Transport Protocol (CRTP)
 - `gr-0/0/0`—Generic routing encapsulation (GRE) and tunneling
 - `ip-0/0/0`—IP-over-IP (IP-IP) encapsulation
 - `pd-0/0/0`, `pe-0/0/0`, and `mt-0/0/0`—All multicast protocols
 - `st0`—Route-based IPsec VPNs
 - `lt-0/0/0`—Real-time performance monitoring (RPM)
- **WXC Integrated Services Module (ISM 200)**
- **Ethernet switching on some PIMs:**
 - 4-port Fast Ethernet ePIMs running in switching mode
 - 8-port and 16-port Gigabit Ethernet uPIMs running in switching mode
- **Some WAN interfaces:**
 - Channelized T1/E1/ISDN PRI
 - ISDN BRI
 - ADSL and SHDSL



NOTE: T1, E1, T3 (DS3), E3, and synchronous serial interfaces *are* supported in chassis cluster configurations.

Outstanding Issues

- ALG** ■ On J6350 Services Routers handling more than 1000 simultaneous MGCP calls, the success rate for all MGCP ALG calls is approximately 95 percent. [PR/254297]
- JUNOS software with enhanced services does not have an option for setting default values for Sun RPC and Microsoft RPC applications. As a workaround, you can define a security policy that specifies a Sun RPC or Microsoft RPC application with the value **any** for the source address, destination address, and application name. [PR/256971]

- Authentication**
- During user authentication, the firewall authentication table in the output of the `security firewall-authentication users` command displays multiple failures even though the network table in the output of `show network-access requests statistics` shows successful authentications. [PR/250780]
 - Your attempt to log in to the router from a management device through FTP or Telnet might fail if you type your username and password in quick succession before the prompt is displayed, in some operating systems. As a workaround, type your username and password after getting the prompts. [PR/255024]
- Chassis Cluster**
- Because the `clear security alg sip call` command triggers a SIP RTO to synchronize sessions in a chassis cluster, use of the command on one node with the `node-id`, `local`, or `primary` option might result in a SIP call being removed from both nodes. [PR/263976]
 - In a chassis cluster configuration, after redundancy group 1 fails over to the secondary node, the statistics for the TCP SYN-ACK-ACK proxy screen are still displayed for the primary node rather than the secondary. [PR/264790]
 - When a new redundancy group is added to a chassis cluster, the node with lower priority might be elected as primary when the `preempt` option is not enabled for the nodes in the redundancy group. [PR/265340]
 - In a chassis cluster, if you manually fail over redundant groups to move the system from active-passive mode to active-active mode during an active call, a subsequent call transfer involving the endpoints of the existing call might fail. [PR/265598]
 - When you commit a configuration for a node belonging to a chassis cluster, all the redundancy groups sometimes fail over to node 0. If graceful protocol restart is not configured, the failover can destabilize routing protocol adjacencies and disrupt traffic forwarding. To allow the commit operation to take place without causing a failover, we recommend that you use the `set chassis cluster heartbeat-threshold 5` command on the cluster. [PR/265801]
 - In a chassis cluster, Layer 2 switching does not work for 4-Port Fast Ethernet ePIMs, 8-Port Gigabit Ethernet uPIMs, and 16-Port Gigabit Ethernet uPIMs. [PR/266857]
 - In a chassis cluster, if a forwarding process restart or system reboot triggers a cold synchronization during an active SIP call, the call might stay in both routing nodes even after the endpoints hang up. As a work around, use the `clear security alg sip call` command to clear the call. [PR/267696]
 - In a chassis cluster, a high load of SIP ALG traffic might result in some call leaks in active resource manager groups and gates on the backup router. [PR/268613]
 - A chassis cluster using Web authentication might display an “invalid username-password” message even though the user is successfully authenticated locally or through authentication servers. To verify user authentication success, use the `show security firewall-authentication users` command. [PR/274077]

- Class of Service**
- 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]
- Flow**
- OSPF over GRE over IPSec does not work. [PR/105279]
 - Even when forwarding options are set to drop packets for the ISO protocol family, the router forms End System-to-Intermediate System (ES-IS) adjacencies and transmits packets because ES-IS packets are Layer 2 terminating packets. [PR/252957]
 - On J-series Services Routers, outbound filters will be applied twice for host-generated IPv4 traffic. [PR/301199]
 - Ping fails when encapsulation `atm-cisco-nlpid` is configured on an interface. As a workaround, disable and then enable the encapsulation. [PR/398864]
- Infrastructure**
- On J-series Services Routers, you cannot use a USB device that provides U3 features (such as the U3 Titanium device from SanDisk Corporation) as the media device during system boot. You must remove the U3 support before using the device as a boot medium. For the U3 Titanium device, you can use the U3 Launchpad Removal Tool on a Windows-based system to remove the U3 features. The tool is available for download at <http://www.sandisk.com/Retail/Default.aspx?CatID=1415>. (To restore the U3 features, use the U3 Launchpad Installer Tool accessible at <http://www.sandisk.com/Retail/Default.aspx?CatID=1411>). [PR/102645]
 - If the router does not have an ARP entry for an IP address, it drops the first packet from itself to that IP address. [PR/233867]
 - 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]
 - If you enable security trace options, the log file might not be created in the default location at `/var/log/security-trace`. As a workaround, manually set the log file to the directory `/var/log/security-trace`. [PR/254563]
- Interfaces and Chassis**
- The link status of the onboard Gigabit Ethernet interfaces (`ge-0/0/0` through `ge-0/0/3`) or the 1-port Gigabit Ethernet ePIM interface on J4350 and J6350 Services Routers fails when you configure these interfaces in loopback mode. [PR/72381]
 - 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]

- Routing** ■ Asymmetric routing, such as tracing a route to a destination behind J-series routers running JUNOS software with enhanced services with Virtual Router Redundancy Protocol (VRRP), does not work. [PR/237589]
- WXC Integrated Services Module** ■ When two J-series routers with WXC Integrated Services Modules (ISM 200s) installed are configured as peers, traceroute fails if `redirect-wx` is configured on both peers. [PR/227958]

Resolved Issues

The following issue has been resolved since Release 9.0R3 of JUNOS software with enhanced services. The identifier following the description is the tracking number in our bug database.

- User Interfaces and Configuration** ■ 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. [PR/94445: This issue has been resolved.]

Errata

- Screens** ■ The following guides contain incorrect screen configuration instructions:
 - *JUNOS Software with Enhanced Services Security Configuration Guide*, “Attack Detection and Prevention” chapter
 - *JUNOS Software with Enhanced Services Design and Implementation Guide*, “Implementing Firewall Deployments for Branch Offices” chapter

Examples throughout both of these guides describe how to configure screen options using the `set security screen screen-name` CLI statements. Instead, you should use the `set security screen ids-option screen-name` CLI statements. All screen configuration options are located in the `[set security screen ids-option screen-name]` level of the configuration hierarchy.

Power and Heat Dissipation Requirements for J-series PIMs

On J-series Services Routers, the system monitors the PIMs and verifies that the PIMs fall within the power and heat dissipation capacity of the chassis. If power management is enabled and the capacity is exceeded, the system prevents one or more of the PIMs from becoming active.



CAUTION: Disabling power management can result in hardware damage if you overload the chassis capacities.

You can also use CLI commands to choose which PIMs are disabled. For details about calculating the power and heat dissipation capacity of each PIM and troubleshooting procedures, see the *JUNOS Software with Enhanced Services Getting Started Guide*.

Supported Third-Party Hardware

The following third-party hardware is supported for use with J-series Services Routers running JUNOS software with enhanced services.

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

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 13 lists the USB and compact flash storage devices supported for use with the J-series Services Routers.

Table 1: Supported Storage Devices on the J-series Services Routers

Manufacturer	Storage Capacity	Third-Party Part Number
SanDisk—Cruzer Mini 2.0	256 MB	SDCZ2-256-A10
SanDisk	512 MB	SDCZ3-512-A10
SanDisk	1024 MB	SDCZ7-1024-A10
Kingston	512 MB	DTI/512KR
Kingston	1024 MB	DTI/1GBKR
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

JUNOS Software with Enhanced Services Upgrade and Downgrade Instructions



NOTE: This information applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software with Enhanced Services Migration Guide*.

In JUNOS Release 8.5, the JUNOS software was extended to use FreeBSD version 6.1. As a result, the following requirements apply when you upgrade your router to JUNOS Release 8.5 and later:

- To upgrade with the JUNOS CLI, the minimum requirement for installation media (such as a compact flash disk, internal flash disk, or PC card) is 256 MB. To use the J-Web interface for an upgrade, you must have 512 MB or more.
- For J-series Services Routers with a 256-MB compact flash:
 - You must perform the upgrade with the CLI. Do not use the J-Web interface for the upgrade.
 - Before upgrading, see the important information in “Special Instructions for J-series Routers with a 256-MB Compact Flash” on page 21.
 - To upgrade without copying the software image to the router—as we recommend—you need at least 68 MB of available space on the compact flash. To copy the software image to the router and upgrade using that image, you need at least 130 MB of available space on the compact flash.

This section contains the following topics.

- Upgrade and Downgrade Overview on page 14
- Before You Begin on page 15
- Downloading Software Upgrades from Juniper Networks on page 16
- Installing Software Upgrades with the J-Web Interface on page 16
- Installing Software Upgrades with the CLI on page 18
- Downgrade Instructions on page 20
- Special Instructions for J-series Routers with a 256-MB Compact Flash on page 21
- Cleaning Up Files on page 22
- Verifying Available Compact Flash Space on page 22
- Removing the Swap Partition on page 23

Upgrade and Downgrade Overview

Typically, you upgrade JUNOS software with enhanced services 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 and JUNOS software with enhanced services 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 signed 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-jsr`.
- *m.n* is the software release, with *m* representing the major release number—for example, `9.0`.
- *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, `1`.
- *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 JUNOS software with enhanced services package name is `junos-jsr-9.0R4-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-cfnnn.gz.

- *package-name* is the name of the package—for example, `junos-jsr`.
- *m.n* is the software release, with *m* representing the major release number—for example, `8.5`.
- *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, `1`.
- `export` indicates that the recovery software package is the exported worldwide software package version.
- *cfnnn* indicates the size of the target compact flash device in megabytes—for example, `cf256`.

A sample JUNOS software with enhanced services recovery package name is `junos-jsr-8.5R1-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 J2320 or J2350 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
```

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/> (customers in the United States and Canada)
 - <https://www.juniper.net/support/csc/swdist-ww/> (all other customers)
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 software with enhanced services image for your application. For information about JUNOS software with enhanced services packages, see “Upgrade and Downgrade Overview” on page 14.
4. Download JUNOS software with enhanced services to a local host or to an internal software distribution site.



NOTE: For downloads to J-series Services Routers with a 256-MB compact flash, see “Special Instructions for J-series Routers with a 256-MB Compact Flash” on page 21.

Installing Software Upgrades with the J-Web Interface

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software upgrades from a remote server using FTP or HTTP, or by uploading the software image to the router. This section contains the following topics:

- Installing Software Upgrades from a Remote Server on page 17
- Installing Software Upgrades by Uploading Files on page 17

Installing Software Upgrades from a Remote Server

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software packages on the router that are retrieved with FTP or HTTP from the location specified. Installing software upgrades using this method copies the software image to the router.



NOTE: This procedure applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software with Enhanced Services Migration Guide*.

To install software upgrades from a remote server:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 16.
2. In the J-Web interface, select **Manage > Software > Install Package**.
3. On the Install Package Quick Configuration page, enter information into the fields described in Table 2 on page 17.
4. Click **Fetch and Install Package**. The software is activated after the router reboots.

Table 2: Install Package 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 server—one of the following: <code>ftp://hostname/pathname/package-name</code> <code>http://hostname/pathname/package-name</code>
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

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software packages uploaded from your computer to the router.



NOTE: This procedure applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software with Enhanced Services Migration Guide*.

To install software upgrades by uploading files:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 16.
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 3 on page 18.
4. Click **Upload Package**. The software is activated after the router has rebooted.

Table 3: Upload Package Summary

Field	Function	Your Action
File to Upload (required)	Specifies the location of the software package on the local system.	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

You can use the CLI to install software upgrades from a remote server using FTP or by downloading the software image to the router. If your router has a 256-MB compact flash, see “Special Instructions for J-series Routers with a 256-MB Compact Flash” on page 21.

This section contains the following topics:

- Installing Software Upgrades by Downloading Files on page 18
- Installing Software Upgrades from a Remote Server on page 19

Installing Software Upgrades by Downloading Files

To install software upgrades by downloading files to the router:

1. Download the JUNOS software with enhanced services package to the router using the following command:

```
user@host> file copy source destination
```

Replace *source* with one of the following paths:

- ftp://hostname/pathname/package-name

or

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

Replace *destination* with the path to the destination directory on the router. We recommend the `/var/tmp` directory.

2. Install the new package on the Services Router, entering the following command in operational mode in the CLI:

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

Replace *source* with `/pathname/package-name` (for example, `/var/tmp/junos-jsr-8.5R2.1.tar.gz`).

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.

3. 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.

Installing Software Upgrades from a Remote Server

To install the software upgrades from a remote server:

1. Install the JUNOS software with enhanced services package on the Services Router, entering the following command in operational mode in the CLI:

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

Replace *source* with 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.

2. 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:

- Downgrading the Software with the J-Web Interface on page 20
- Downgrading the Software with the CLI on page 21



NOTE: Juniper Networks supports direct software downgrades for a maximum of three releases.

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.



NOTE: This procedure applies only to downgrading one release of JUNOS software with enhanced services to another. To downgrade JUNOS software with enhanced services to the JUNOS software, see the *JUNOS Software with Enhanced Services Migration Guide*.

To downgrade software with the J-Web interface:

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, click **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 software image of JUNOS software with enhanced services 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 software image of JUNOS software with enhanced services labeled with the appropriate release.



NOTE: This procedure applies only to downgrading one release of JUNOS software with enhanced services to another. To downgrade JUNOS software with enhanced services to the JUNOS software, see the *JUNOS Software with Enhanced Services Migration Guide*.

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. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image of JUNOS software with enhanced services labeled with the appropriate release.

Special Instructions for J-series Routers with a 256-MB Compact Flash

J-series Services Routers with a 256-MB compact flash might need more flash memory space for an upgrade.

To provide enough space for an upgrade:

- Clean up files on the router (see “Cleaning Up Files” on page 22).
- Verify the available compact flash space (see “Verifying Available Compact Flash Space” on page 22).

- If required, increase the compact flash space, (see “Removing the Swap Partition” on page 23).

Cleaning Up Files

To clean up files, you use CLI commands to delete the backup software image, rotate log files, and remove other unnecessary files.

When you upgrade software on the router, it creates a backup image of the software that was previously installed. To create enough space on a 256-MB compact flash for an upgrade, use the `request system software delete-backup` command to delete this image. In addition, use the `request system storage cleanup` command to rotate log files and delete unnecessary files.



NOTE: To review the list of files that can be deleted without actually deleting files, you can use the `request system storage cleanup dry-run` command.

To delete the backup software image, rotate log files, and delete unneeded files:

1. From operational mode in the CLI, enter the following command:

```
user@host> request system software delete-backup
```

2. Enter `yes` when prompted:

```
Delete backup system software package [yes,no] (no) yes
```

3. Enter the following command:

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

The router rotates log files and displays the files that you can delete.

4. Enter `yes` at the prompt to delete the files.
5. Delete any files that you created by entering the following command:

```
user@host> file delete filename
```

Replace *filename* with the name of the file or directory to delete.

6. Verify that you have enough space on the compact flash to successfully upgrade (see “Verifying Available Compact Flash Space” on page 22).

Verifying Available Compact Flash Space

Before you start the upgrade, verify that you have enough space on the compact flash to successfully upgrade.

To see how much space is available on the compact flash, use the CLI operational mode command `show system storage`:

```

user@host show system storage
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/ad0s1a     213M     119M      92M    57%      /
devfs           1.0K     1.0K      0B     100%    /dev
devfs           1.0K     1.0K      0B     100%    /dev/
/dev/md0        155M     155M      0B     100%    /junos
/cf             213M     119M      92M    57%    /junos/cf
devfs           1.0K     1.0K      0B     100%    /junos/dev/
procfs          4.0K     4.0K      0B     100%    /proc
/dev/bo0s1e     24M      16K      24M     0%    /config
/dev/md1        168M     7.2M     147M     5%    /mfs
/dev/md2         58M      42K      53M     0%    /jail/tmp
/dev/md3         7.7M    100K      7.0M     1%    /jail/var/etc
devfs           1.0K     1.0K      0B     100%    /jail/dev
/dev/md4         1.9M     6.0K     1.7M     0%    /jail/html/oem

```

The `show system storage` command output displays information about the root file system on the compact flash on the line that contains only a forward slash (/) in the **Mounted on** column. In this example, the compact flash has 92 MB of available space.

If the `show system storage` command output displays:

- Available compact flash space—135 MB or more. See “Installing Software Upgrades with the CLI” on page 18 to proceed with the upgrade.
- Available compact flash space—less than 135 MB. See “Removing the Swap Partition” on page 23 to increase the compact flash space.

Removing the Swap Partition



NOTE: On J-series Services Routers running JUNOS Release 8.2 or later, you can no longer specify the internal compact flash as the medium used to store system software failure memory snapshots when using the `set system dump-device` CLI command. For J4350 or J6350 Services Routers, you need to specify a USB storage device (`usb` option) as the medium. For J2320 and J2350 Services Routers, you can specify a USB storage device (`usb` option) or the external compact flash (`removable-compact-flash` option) as the medium.

To increase the compact flash space, remove the swap partition:

1. Insert a Juniper Networks-supported 256-MB USB storage device into an available USB port of the Services Router to be upgraded. See “Supported Third-Party Hardware” on page 13 for a list of supported storage devices.
2. From operational mode in the CLI, enter the following command:

```

user@host> request system snapshot as-primary partition swap-size 0 media
usb

```

3. Enter the following command:

```

user@host> request system reboot media usb

```

This command reboots the router and boots from the USB storage device with the original configuration file intact. After rebooting, the router is online and uses the configuration file as the running configuration.

4. Enter the following command:

```
user@host> request system snapshot as-primary partition swap-size 0 media compact-flash
```

This command repartitions the internal compact flash so that it has no swap partition.

5. Enter the following command:

```
user@host> request system reboot media compact-flash
```

This command reboots the router from the internal compact flash. After rebooting, the router is online with your running configuration, but the swap partition on the compact flash is removed.

6. Remove the USB storage device.
7. See “Installing Software Upgrades with the CLI” on page 18 to proceed with the upgrade.

List of Technical Publications

Table 4 on page 24 lists the software and hardware guides and release notes for Juniper Networks J-series, M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 5 on page 28 lists the books included in the *Network Operations Guide* series. Table 6 on page 29 lists the manuals and release notes supporting JUNOS software with enhanced services. All documents are available at <http://www.juniper.net/techpubs/>.

Table 7 on page 30 lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at <http://www.juniper.net/books>.

Table 4: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	
<i>Access Privilege</i>	Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements.
<i>Class of Service</i>	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.

Table 4: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>CLI User Guide</i>	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 <i>JUNOS System Basics Configuration Guide</i> .
<i>Feature Guide</i>	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
<i>High Availability</i>	Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop active routing (NSR) and graceful Routing Engine switchover (GRES).
<i>MPLS Applications</i>	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
<i>Multicast Protocols</i>	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
<i>Multiplay Solutions</i>	Describes how you can deploy IPTV and voice over IP (VoIP) services in your network.
<i>MX-series Solutions Guide</i>	Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB).
<i>Network Interfaces</i>	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
<i>Protected System Domain</i>	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.

Table 4: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i>	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
<i>Software Installation and Upgrade Guide</i>	Describes the JUNOS software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>System Basics</i>	Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
<i>VPNs</i>	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.
JUNOS References	
<i>Hierarchy and RFC Reference</i>	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 <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
<i>System Basics and Services Command Reference</i>	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. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	

Table 4: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
<i>JUNOS XML API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
<i>NETCONF API Guide</i>	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	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.
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
<i>PIC Guide</i>	Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide.
<i>DPC Guide</i>	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
Advanced Insight Solutions (AIS) Documentation	
<i>Advanced Insight Solutions Guide</i>	Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI scripts on Juniper Networks devices.
J-series Routing Platform Documentation	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series routing platforms. 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 <i>Getting Started Guide</i> for your router model.
<i>Basic LAN and WAN Access Configuration Guide</i>	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.

Table 4: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>Advanced WAN Access Configuration Guide</i>	Explains how to configure J-series Services Routers 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.
<i>Administration Guide</i>	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Release Notes	
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
<i>Hardware Release Notes</i>	Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope Release Notes</i>	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.
<i>AIS Release Notes</i>	Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.
<i>AIS AI Script Release Notes</i>	Summarize AI Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.
<i>J-series Services Router Release Notes</i>	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 5: JUNOS Software Network Operations Guides

Book	Description
<i>Baseline</i>	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
<i>Interfaces</i>	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.

Table 5: JUNOS Software Network Operations Guides (continued)

Book	Description
<i>MPLS</i>	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
<i>MPLS Log Reference</i>	Describes MPLS status and error messages that appear in the output of the <code>show mpls lsp extensive</code> command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.
<i>MPLS Fast Reroute</i>	Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing.
<i>Hardware</i>	Describes tasks for monitoring M-series and T-series routing platforms.

To configure and operate a J-series Services Router running JUNOS software with enhanced services, you must also use the configuration statements and operational mode commands documented in JUNOS configuration guides and command references. To configure and operate a WX Integrated Services Module, you must also use WX documentation.

Table 6: JUNOS Software with Enhanced Services Documentation

Book	Description
All Platforms	
<i>JUNOS Software Interfaces and Routing Configuration Guide</i>	Explains how to configure J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
<i>JUNOS Software Security Configuration Guide</i>	Explains how to configure and manage security services such as stateful firewall policies, IP Security (IPsec) virtual private networks (VPNs), firewall screens, Network Address Translation (NAT), Public Key Cryptography, and Application Layer Gateways (ALGs).
<i>JUNOS Software Administration Guide</i>	Shows how to monitor J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
<i>JUNOS Software CLI Reference</i>	Provides the complete JUNOS software with enhanced services configuration hierarchy and describes the configuration statements and operational mode commands not documented in the standard JUNOS manuals.

Table 6: JUNOS Software with Enhanced Services Documentation (continued)

Book	Description
J-series Only	
<i>JUNOS Software with Enhanced Services Design and Implementation Guide</i>	Provides guidelines and examples for designing and implementing IP Security (IPsec) virtual private networks (VPNs), firewalls, and routing on J-series Services Routers running JUNOS software with enhanced services.
<i>JUNOS Software with Enhanced Services Quick Start</i>	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
<i>JUNOS Software with Enhanced Services Migration Guide</i>	Provides instructions for migrating an SSG device running ScreenOS software or a J-series Services Router running the JUNOS software to JUNOS software with enhanced services.
<i>WXC Integrated Services Module Installation and Configuration Guide</i>	Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.
<i>JUNOS Software with Enhanced Services Release Notes</i>	Summarizes new features and known problems for a particular release of JUNOS software with enhanced services on J-series Services Routers, including J-Web interface features and problems. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software with enhanced services.

Table 7: Additional Books Available Through <http://www.juniper.net/books>

Book	Description
<i>Interdomain Multicast Routing</i>	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.
<i>JUNOS Cookbook</i>	Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs.
<i>MPLS-Enabled Applications</i>	Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks.

Table 7: Additional Books Available Through <http://www.juniper.net/books> (continued)

Book	Description
<i>OSPF and IS-IS: Choosing an IGP for Large-Scale Networks</i>	Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks.
<i>Routing Policy and Protocols for Multivendor IP Networks</i>	Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers.
<i>The Complete IS-IS Protocol</i>	Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach.

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 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 Management tool: <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 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, 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](ftp://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 <https://www.juniper.net/cgi-bin/docbugreport/>.

Revision History

November 2008—Revision 4, JUNOS Software Release 9.0R4

August 2008—Revision 3, JUNOS Software Release 9.0R3

March 2008—Revision 2, JUNOS Software Release 9.0R2

14 February 2008—Revision 1, JUNOS Software Release 9.0R1

Copyright © 2008, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS is a trademark 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.