

JUNOScope 10.0 Software Release Notes

Release 10.0R4
24 August 2010
Revision 4

These release notes accompany Release 10.0R4 of the JUNOS Software. They describe the key features, documentation, and known problems with the software. The JUNOScope software is a network management application that provides router configuration management, inventory management, software management, operation status, and troubleshooting tools for Juniper Networks J-series, M-series, MX-series, and T-series routing platforms.

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

Contents

Release 10.0 Features	3
Current Software Release	4
JUNOScope Software Usage Guidelines	4
Install Latest Appropriate Operating System Patches	4
Verify the JUNOScope Image Against Values Published on the Juniper Networks Web Site	5
Upgrading JUNOScope and Password Policies	5
Protecting JUNOScope Data Files	5
Always Use Strong Passwords	5
Change the Default Install Time User from 'admin' to Another Name	6
Disable Access to the Inventory Management System SQL Interface	6
Do Not Enable Debugging on JUNOScope at Installation	6
Use Only HTTPS to Connect from a Browser Client to the JUNOScope Server	6
Use Only SSL to Connect from the JUNOScope Software to Network Devices	7
Do Not Export JUNOScope Data in Clear Text or with the Encryption Key in the Exported Data	7
Disable User Accounts After Login Failure Attempts Within The Time Window Are Exceeded	7
Regularly Back Up the JUNOScope Software Server	7
Installing the JUNOScope Software	7
System Requirements	8
Red Hat Enterprise Linux ES File Package Requirements	8

JUNOScope Client Workstation Requirements	9
RADIUS Server Requirements	9
Syslog Server Requirements	9
Installing the JUNOScope Software	9
Downloading the JUNOScope Software from the Software Download Page	10
Reconfiguring the JUNOScope Software	10
Reinstalling or Upgrading the JUNOScope Software	11
Uninstalling the JUNOScope Software	11
List of Technical Publications	11
Documentation Feedback	15
Requesting Technical Support	16
Self-Help Online Tools and Resources	16
Opening a Case with JTAC	16
Revision History	17

Release 10.0 Features

The following features have been added to JUNOScope Release 10.0. For more detailed information, see the appropriate sections of the *JUNOScope Software User Guide*.

- **Support for Layer 2 Virtual Packet Network (Layer 2 VPN) Pseudowires:** Starting Release 10.0, JUNOScope extends its support to the provisioning of BGP-based Layer 2 VPN pseudowires for devices in JUNOScope. The provisioning Layer 2 VPN pseudowires workflow consists of two main tasks: Provisioning Layer 2 VPN Pseudowires, and Filtering and Testing Layer 2 VPN Pseudowires. To use these features, go to the Provisioning l2vpn Pseudowires (Provisioning > Pseudowires > Provisioning l2vpn Pseudowires), and the Filter and Test l2vpn Pseudowires Wizard (Provisioning > Pseudowires > Filter and Test l2vpn Pseudowires).

JUNOScope also enables you to generate a stitching configuration that connects an LDP-based Layer 2 circuit pseudowire with a BGP-based Layer 2 VPN pseudowire, and push the generated configuration to a selected device. You can create a stitching configuration between two Layer 2 VPN pseudowires, two Layer 2 circuit pseudowires, or between an Layer 2 circuit pseudowire and an Layer 2 VPN pseudowire. To use this feature, go to the Stitching l2circuit > l2vpn Wizard (Provisioning > Pseudowires > Stitching l2circuit > l2vpn).

For more information, see *JUNOScope Software User Guide*.

- **Monitoring Pseudowires:** Starting Release 10.0, JUNOScope enables you to monitor traffic and set an alarm when a certain condition occurs. It involves two main steps:
 - Configure the devices in JUNOScope with the SNMP trap destination — SNMP trap destinations define the hosts that will receive the SNMP traps that are generated by the trap group when certain conditions apply. This way, JUNOScope is notified about each object on its managed devices without having to request for any information.
 - Create templates of Remote Monitoring (RMON) events for which the traps are generated — SNMP makes use of Remote Monitoring (RMON) enhancements to the management information base (MIB) structure to monitor traffic and set an alarm when a certain condition occurs.

You can also view important attributes of a pseudowire such as jitter, delay, packet loss, etc. To use this feature, go to the Monitor Pseudowires Wizard (Provisioning > Pseudowires > Monitoring).

For more information, see *JUNOScope Software User Guide*.

- **Support for Diagnostic Tests:** Starting Release 10.0, JUNOScope enables you to diagnose routing problems by running diagnostic commands. These diagnostic commands allow you to capture and analyze routing platform control traffic.

JUNOScope supports the following diagnostic commands:

- Ping — Ping is used to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems.
- LSP Ping — LSP ping is used to isolate and identify faults in an MPLS-based network.
- Traceroute — Traceroute is used to display a list of routers that exist between the device and a specified destination host. This output is useful for diagnosing a point of failure in the path from the device to the destination host, and addressing the network traffic latency and throughput problems.
- BERT Test — Bit Error Rate Testing is used to test the quality of links.

For more information, see *JUNOScope Software User Guide*.

Current Software Release

The current JUNOScope software release is Release 10.0R4. For information about installing the software release, see “Installing the JUNOScope Software” on page 9.

JUNOScope Software Usage Guidelines

- Install Latest Appropriate Operating System Patches on page 4
- Verify the JUNOScope Image Against Values Published on the Juniper Networks Web Site on page 5
- Upgrading JUNOScope and Password Policies on page 5
- Protecting JUNOScope Data Files on page 5
- Always Use Strong Passwords on page 5
- Change the Default Install Time User from ‘admin’ to Another Name on page 6
- Disable Access to the Inventory Management System SQL Interface on page 6
- Do Not Enable Debugging on JUNOScope at Installation on page 6
- Use Only HTTPS to Connect from a Browser Client to the JUNOScope Server on page 6
- Use Only SSL to Connect from the JUNOScope Software to Network Devices on page 7
- Do Not Export JUNOScope Data in Clear Text or with the Encryption Key in the Exported Data on page 7
- Disable User Accounts After Login Failure Attempts Within The Time Window Are Exceeded on page 7
- Regularly Back Up the JUNOScope Software Server on page 7

Install Latest Appropriate Operating System Patches

Apply all appropriate operating system (such as Solaris or Linux) patches to keep the JUNOScope server less vulnerable to discovered exploits. Regularly check for and install updates. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Verify the JUNOScope Image Against Values Published on the Juniper Networks Web Site

To ensure the authenticity of the JUNOScope software, compare the hash value of the JUNOScope image with the MD5 or SHA-1 hash values posted on the Juniper Networks Web site at <https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/>. You can validate the JUNOScope image obtained by HTTPS download, for example, `jtk-install-10.0R4-sunos5.sh` for Solaris.

To generate the hash value, use the following command:

```
hostname% openssl dgst10.0R4-openssl dgst jtk-install-10.0R4-sunos5.sh
```

Upgrading JUNOScope and Password Policies

When upgrading from JUNOScope 8.1 or earlier, the password policy is not enforced on any existing user accounts. It is recommended that the administrator change the password for existing user accounts in order to comply with the password policy.

Protecting JUNOScope Data Files

During the JUNOScope software installation, you are asked to specify how you want to protect JUNOScope data files. The available options are user, group, and all. Select the User option to specify that only the user who installed the JUNOScope software can read JUNOScope data files.

Always Use Strong Passwords

The initial **admin** account, created at install time, should have an extra-strong password as it cannot be disabled through repeated login failures. The password for the administrator should not match the username, and should not be a word that can be easily guessed.

In general, JUNOScope software passwords must be:

- Easy to remember so that users are not tempted to write them down.
- Contain between 6 and 128 characters, using at least two of the four defined character sets (uppercase, lowercase, numeric, other). The characters in the set "other" are those that can be entered using a single keystroke, or a keyboard character accessed using the Shift key, that does not fall into any of the other three groups.
- Changed periodically.
- Not divulged to anyone.

Weak passwords are:

- Words that might be found in or exist as a permuted form in system files such as `/etc/passwd`.
- The hostname of the system (always a first guess).
- Any word that appears in a dictionary. This includes dictionaries other than English, and words found in works such as Shakespeare, Lewis Carroll, Roget's Thesaurus, and

so on. This prohibition includes common words and phrases from sports, sayings, movies, or television shows.

- Permutations of any of the above. For example, a dictionary word with vowels replaced with digits (f00t) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and should not be used.

Strong reusable passwords can be:

- Based on letters from a favorite phrase or word, and
- Concatenated with other, unrelated words, along with added digits and punctuation.

Passwords should be changed from time to time. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Change the Default Install Time User from ‘admin’ to Another Name

The JUNOScope administrative default user account name is **admin**. The JUNOScope installation creates this initial JUNOScope administrative user account so the administrator can use it to add other users. Change the default user account name to another name during the installation process. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Disable Access to the Inventory Management System SQL Interface

During the JUNOScope software installation, you are asked to confirm whether you want to enable access to the Inventory Management System SQL interface. The default is **no**. If you select **no**, the SQL interface cannot be accessed by any other application or host except JUNOScope clients. If you select **yes**, the MySQL database can be accessed by any application with Inventory Management System user credentials.

Do Not Enable Debugging on JUNOScope at Installation

The JUNOScope software installation confirms whether you want to enable debug logging for technical support purposes. The default and recommended setting is **no**. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Use Only HTTPS to Connect from a Browser Client to the JUNOScope Server

The JUNOScope software accepts Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS).

The JUNOScope software provides security between the client and the server. MD5 RSA certification is available between the JUNOScope server and the client Web browser. All communication is encrypted between the client Web browser and the JUNOScope server. The JUNOScope software installation creates an X.509 digital certificate to authenticate the HTTPS server. The JUNOScope software administrator can use self-assigned certificates, or have one assigned by a trusted certificate authority.

The JUNOScope software installation prompts for the HTTPS port that the JUNOScope software Web server uses for its transactions. It is recommended that you use the HTTPS port for communication between the JUNOScope Web browsers and the JUNOScope server. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Use Only SSL to Connect from the JUNOScope Software to Network Devices

The JUNOScope software uses the SSL JUNOScript access protocol to connect to configured devices on the network. The SSL protocol is preferred because it encrypts security information (such as a password) before transmitting it across the network. For more information about how to use the SSL access protocol to connect to devices, see the *JUNOScope Software User Guide*, “Setting Up Access Methods” chapter.

Do Not Export JUNOScope Data in Clear Text or with the Encryption Key in the Exported Data

When exporting sensitive data in authentication information from the JUNOScope software server, use the **Encrypt sensitive data and provide key at import time** export option. Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import. For more information about exporting all data from the JUNOScope server, see the *JUNOScope Software User Guide*, “Importing and Exporting All Settings Data” chapter, or the specific JUNOScope operation chapter export section.

Disable User Accounts After Login Failure Attempts Within The Time Window Are Exceeded

Configure a Global User Authentication Policy to disable user accounts after the login failure attempts within the time window, as defined by the administrator, has been exceeded. Enable the global user authentication policy; it is disabled by default. For more information about creating global authentication policies, see the *JUNOScope Software User Guide*, “Setting Up a Global Authentication Policy” chapter.

Regularly Back Up the JUNOScope Software Server

Perform regular backups of application data stored by JUNOScope to prevent data loss in the event of a disaster. For more information about backing up JUNOScope application data, see the *JUNOScope Software User Guide*, “Backing Up and Restoring the JUNOScope Application Data” chapter.

Installing the JUNOScope Software

This section describes how to install, reconfigure, reinstall, upgrade, and uninstall the JUNOScope software.

Before installing the JUNOScope software, ensure that your network meets the requirements described in the following sections:

- System Requirements on page 8
- Red Hat Enterprise Linux ES File Package Requirements on page 8
- JUNOScope Client Workstation Requirements on page 9
- RADIUS Server Requirements on page 9

- Syslog Server Requirements on page 9
- Installing the JUNOScope Software on page 9
- Reconfiguring the JUNOScope Software on page 10
- Reinstalling or Upgrading the JUNOScope Software on page 11
- Uninstalling the JUNOScope Software on page 11

System Requirements

The JUNOScope software runs on both Sun Solaris servers (see Table 1 on page 8) and Red Hat Linux servers (see Table 2 on page 8). Before you install the JUNOScope software, ensure that the supported UNIX server workstation on which you install the software meets the following system requirements.

Table 1 on page 8 shows the minimum system requirements for a Sun Solaris server.

Table 1: Sun Solaris Server System Minimum Requirements

System	Minimum Requirement
Operating system	Solaris 5.8 or later
Processor	UltraSPARC III or equivalent
Speed	1.3 GHz or faster
RAM	1 GB
Free disk space	1 GB

Table 2 on page 8 shows the minimum system requirements for a Red Hat Linux server. (See also Table 3 on page 9).

Table 2: Red Hat Linux Server System Minimum Requirements

System	Minimum Requirement
Hardware	Red Hat certified hardware platforms
Operating system	Red Hat Enterprise Linux ES version 3 and 4
Processor	Pentium 4 processor
Speed	2.8 GHz or faster
RAM	1 GB
Free disk space	1 GB

Red Hat Enterprise Linux ES File Package Requirements

If a minimal install of Red Hat Enterprise Linux ES is performed on the server, the JUNOScope software administrator should ensure that the following file packages are

installed for the JUNOScope software to run properly (see Table 3 on page 9. All packages should be available in a full install of Red Hat Enterprise Linux ES.

Table 3: Red Hat Enterprise Linux ES File Package Requirements

Version	Required File Packages
Red Hat Enterprise Linux ES version 3 (Update 6)	krb5-libs-1.2.7-47.i386.rpm XFree86-libs-4.3.0-97.EL.i386.rpm
Red Hat Enterprise Linux ES version 4 (Update 2)	compat-libcom_err-1.0-5.i386.rpm krb5-libs-1.3.4-17.i386.rpm xorg-x11-deprecated-libs-6.8.2-1.EL.13.20.i386.rpm xorg-x11-libs-6.8.2-1.EL.13.20.i386.rpm

To verify that the file package `krb5-libs-1.3.4-17.i386.rpm` is installed, use the following command:

```
hostname% rpm --queryformat "%{NAME}-%{VERSION}-%{RELEASE}-%{ARCH}\n"
--query krb5-libs
```

You can install each package individually via `rpm`, from the original Red Hat Enterprise Linux ES distribution. To install the file package `xorg-x11-libs-6.8.2-1.EL.13.20.i386.rpm`, use the following command:

```
hostname% rpm --install xorg-x11-libs-6.8.2-1.EL.13.20.i386.rpm
```

JUNOScope Client Workstation Requirements

Ensure that the client workstation from which you connect to the JUNOScope software is running either Microsoft Internet Explorer 6 or Netscape Navigator 6 or later with JavaScript enabled.

RADIUS Server Requirements

Ensure that the RADIUS server complies with *RFC 2865, Remote Authentication Dial-In User Service*.

Syslog Server Requirements

Ensure that the system server (`syslog`) is running and configured to receive JUNOScope system log messages.

Installing the JUNOScope Software

This section describes how to install the JUNOScope Software from the JUNOScope software download page. For more information about installing the JUNOScope software, see the *JUNOScope Software User Guide*.

- Downloading the JUNOScope Software from the Software Download Page on page 10

Downloading the JUNOScope Software from the Software Download Page

To download the JUNOScope software from the Juniper Networks Web site and start the JUNOScope installation, follow these steps:

1. Using a Web browser, go to the following location:

<https://www.juniper.net/junos/swdist/encryption/index.htm>

2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
3. Download the appropriate JUNOScope software to the server workstation.
4. Start the JUNOScope installation program:

```
hostname% download-directory/jtk-install-10.0R4.X-sunos5-sparc.sh install-directory  
or  
hostname% download-directory/jtk-install-10.0R4.X-linux2-i386.sh install-directory
```

Replace **download-directory** with the directory into which you downloaded the JUNOScope software from the software download page.

jtk-install-10.0R4.X-sunos5-sparc.sh or jtk-install-10.0R4.X-linux2-i386.sh is the JUNOScope software file. Where *X* is the current software spin number.

Replace **install-directory** with the directory in which to install the JUNOScope software. If you do not specify an installation directory, the software is installed in the current directory.

Reconfiguring the JUNOScope Software

You can change the following JUNOScope software installation settings without rerunning the installation program. For more information about these settings, see the *JUNOScope Software User Guide*.

- HTTPS and HTTP ports on which the JUNOScope Web server should listen
- Port on which the JUNOScope server listens for control messages
- HTTP port on which the JUNOScope report server should listen
- Java Database Connectivity (JDBC) URL for accessing the JUNOScope database and demo database
- Enable or disable access for SQL interface to Inventory Management System
- Debug logging
- Syslog facility
- Idle session timeout
- Licensed software modules

You cannot change some settings, such as passwords. To change JUNOScope software settings, use the following command:

```
hostname%install-directory/jtk/bin/jtk-setup.sh
```

Reinstalling or Upgrading the JUNOScope Software

The process for reinstalling or upgrading the JUNOScope software is the same as for installing the software. To install the JUNOScope software, see “Downloading the JUNOScope Software from the Software Download Page” on page 10.

To reinstall or upgrade JUNOScope software, you must use the same user ID as the one used for the currently installed software.

Uninstalling the JUNOScope Software

To uninstall the JUNOScope software, follow these steps:

1. Stop the JUNOScope software and database by changing to the directory where you installed the JUNOScope software and typing the following command:

```
hostname% install-directory/jtk/rc.d/jtk stop
```

2. Remove the JUNOScope software by typing the following command:

```
hostname% rm-rf install-directory
```



WARNING: The `rm-rf install-directory` command removes the JUNOScope `install-directory`, including all data.

List of Technical Publications

Table 4 on page 11 lists the software and hardware guides and release notes for Juniper Networks M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 5 on page 12 lists the books included in the *Network Operations Guide* series. Table 6 on page 13 lists the manuals and release notes supporting Junos OS for J-series and SRX-series platforms. All documents are available at <http://www.juniper.net/techpubs/>.

Table 7 on page 15 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
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.

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

Book	Description
<i>DPC Guide</i>	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
Junos Scope Documentation	
<i>Junos Scope Software User Guide</i>	Describes the Junos Scope 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.
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, Junos XML protocol, 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>Junos Scope Release Notes</i>	Contain corrections and updates to the published Junos Scope 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-Scripts 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.

Table 5: Junos OS 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 OS, gathering basic system management information, verifying your network topology, and searching log messages.

Table 5: Junos OS Network Operations Guides (*continued*)

Book	Description
<i>Interfaces</i>	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
<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 or an SRX-series Services Gateway running Junos OS, 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 OS for J-series Services Routers and SRX-series Services Gateways Documentation

Book	Description
J-series and SRX-series Platforms	
<i>Junos OS Interfaces and Routing Configuration Guide</i>	Explains how to configure SRX-series and 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 OS Security Configuration Guide</i>	Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP).

Table 6: Junos OS for J-series Services Routers and SRX-series Services Gateways Documentation (*continued*)

Book	Description
<i>Junos OS Administration Guide for Security Devices</i>	Shows how to monitor SRX-series and 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 OS CLI Reference</i>	Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices.
<i>Network and Security Manager: Configuring J Series Services Routers and SRX Series Services Gateways Guide</i>	Explains how to configure, manage, and monitor J-series Services Routers and SRX-series services gateways through NSM.
<i>Junos Release Notes</i>	Summarize new features and known problems for a particular release of Junos OS, including Junos OS for J-series and SRX-series devices. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for Junos OS.
J-series Only	
<i>Junos OS Design and Implementation Guide</i>	Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running Junos OS.
<i>J Series Services Routers 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 J-series Services Router Hardware Guide</i>	Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.
<i>Junos OS Migration Guide</i>	Provides instructions for migrating an SSG device running ScreenOS software to Junos OS or upgrading a J-series device to a later version of the Junos OS.
<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.

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 OS 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.
<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 <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or 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/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <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: <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>

Revision History

26 October 2009 —R1 JUNOS 10.0

15 December 2009 —R2 JUNOS 10.0

19 April 2010 —R3 JUNOS 10.0

24 August 2010 —R4 JUNOS 10.0

Copyright © 2010, Juniper Networks, Inc. All rights reserved.

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

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

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.