

JUNOScope 9.5 Software Release Notes

Release 9.5R4
19 February 2010
Part Number: 530-029335-01
Revision R4

These release notes accompany Release 9.5R4 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 9.5 Features	3
Current Software Release	5
Outstanding Issue	5
JUNOScope Software Usage Guidelines	5
Install Latest Appropriate Operating System Patches	6
Verify the JUNOScope Image Against Values Published on the Juniper Networks Web Site	6
Upgrading JUNOScope and Password Policies	6
Protecting JUNOScope Data Files	6
Always Use Strong Passwords	6
Change the Default Install Time User from 'admin' to Another Name	7
Disable Access to the Inventory Management System SQL Interface	8
Do Not Enable Debugging on JUNOScope at Installation	8
Use Only HTTPS to Connect from a Browser Client to the JUNOScope Server	8
Use Only SSL to Connect from the JUNOScope Software to Network Devices	8

Do Not Export JUNOScope Data in Clear Text or with the Encryption Key in the Exported Data	8
Disable User Accounts After Login Failure Attempts Within The Time Window Are Exceeded	9
Regularly Back Up the JUNOScope Software Server	9
Installing the JUNOScope Software	9
System Requirements	9
Red Hat Enterprise Linux ES File Package Requirements	10
JUNOScope Client Workstation Requirements	11
RADIUS Server Requirements	11
Syslog Server Requirements	11
Installing the JUNOScope Software	11
Downloading the JUNOScope Software from the Software Download Page	12
Reconfiguring the JUNOScope Software	12
Reinstalling or Upgrading the JUNOScope Software	13
Uninstalling the JUNOScope Software	13
List of Technical Publications	13
Documentation Feedback	20
Requesting Technical Support	20
Self-Help Online Tools and Resources	21
Opening a Case with JTAC	21
Revision History	21

Release 9.5 Features

The following features have been added to JUNOScope Release 9.5. For more detailed information, see the appropriate sections of the *JUNOScope Software User Guide*.

- **Extension of the Software Manager functionality:**
 - **Verification of MD5 checksum of downloaded and imported software images:** Starting Release 9.5, JUNOScope enables you to verify if the downloaded software image is intact by selecting the **Verify MD5 Checksum for downloaded image** option on the Download Image wizard. You can enter the MD5 checksum value in the **MD5 Checksum For Verification** field in the Images Import wizard. The checksum value can be obtained from <http://www.juniper.net/customers/support/>. If you select this option, the checksum of the imported or downloaded software image is compared with the checksum that is stored in JUNOScope. If they do not match, the image download or import operation fails and an error message “MD5 checksum of downloaded image does not match the image in JUNOScope” is displayed on the status page. To enable this option, select the **Verify MD5 Checksum for downloaded image** option provided on the Download Image wizard (Software Management > Images > Download Image).
 - **Support of multiple Routing Engine systems:** Starting Release 9.5, JUNOScope extends its support of dual routing engine systems by enabling you to select the routing engine (RE) on which the software image is to be installed. In case of dual routing engine systems, you can select the routing engine from a list that is displayed on the JUNOScope Software Management Image Installing wizard (Software Management > Images > Install). The options provided are Current RE, Master RE, and Backup RE. The Current RE option is selected by default. You can also install downloaded images from the Current RE, the Master RE, or the Backup RE.
 - **Support of multiple protocols for image transfer to device:** Starting Release 9.5, JUNOScope enables you to select the protocol to be used for image transfer. You can select FTP, SCP, or HTTP to transfer a file. HTTP is selected by default. To use this feature, select a protocol listed in the **Select Transfer protocol:** list that is provided on the JUNOScope Software Management Image Downloading wizard (Software Management > Images > Download).

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

- **Extension of the Operation Script functionality:**

- **Verification of MD5 checksum of imported and downloaded scripts:** Starting Release 9.5, JUNOScope enables you to verify if the downloaded script is intact by selecting the **Verify MD5 Checksum for downloaded script** option on the Download Script wizard. You can enter the MD5 checksum value in the **MD5 Checksum For Verification** field in the Script Import wizard. The checksum value can be obtained from <http://www.juniper.net/customers/support/>. If you select this option, the checksum of the imported or downloaded script is checked against the checksum that is stored in JUNOScope. If they do not match, the script download or import operation fails and an error message “MD5 checksum of downloaded script does not match the script in JUNOScope” is displayed on the status page. To enable this option, select the **Verify MD5 Checksum for downloaded script** option provided on the JUNOScope Script wizard (Configuration > Repository > Scripts).
- **Support of script deployment on multiple Routing Engine systems:** Starting Release 9.5, JUNOScope extends its support of dual routing engine systems by enabling you to select whether you want to deploy the script on both routing engine systems. To enable this feature, select the **Deploy on Both REs (in case of dual RE)** option in the JUNOScope Script wizard (Configuration > Repository > Scripts).
- **Support of Operation Script Execution:** Starting Release 9.5, JUNOScope enables you to execute a deployed operation script. To execute a selected operation script, first select the revision and specify the parameters for the script execution on the Execute Script wizard (Configuration > Repository > Scripts > Execute). Then, select the group or devices on which the script should be executed. Finally, select whether you want the script to be executed immediately, if you want to save the operation for later use, or if you want the script execution to occur at a scheduled time. The status page (Monitor > Status > View Status Record) will change. The operation script will have a new link **View Output** displayed under the Action column. Click **View Output** to view the results of the operation script execution.
- **Support of multiple protocols for script transfer to device:** Starting Release 9.5, JUNOScope enables you to select the protocol that should be used for script transfer. You can select FTP, SCP, or HTTP to deploy a script. HTTP is selected by default. To use this feature, select a protocol from the list in the **Upload Protocol** drop-down list that is provided in the JUNOScope Script Deploy wizard (Configuration > Repository > Scripts > Deploy > Step 2: Specify devices and time).

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

- **Enhancement of JUNOScope functionality to support the assigning of devices to saved operations:** Starting Release 9.5, JUNOScope enables you to assign devices or a group to a saved operation. The saved operation is used as a template but it will not run on the devices that were originally specified in the saved operation. The saved operations will instead run on the new devices that you specified. . To assign a device or group to a saved operation, go to the Assign Device for running Saved Operations dialog box (Setting > Saved Operations > Assign devices to Saved Operations). In this dialog box, you can select the groups or devices that you want to assign to the saved operation; then select whether you want the operation to run now, save it for future use, or run at a scheduled time.

For a sequential task that involves an image upgrade, you can simultaneously execute the task on a maximum of 25 devices.

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

- **Enhancement of JUNOScope functionality to support the re-synchronization of device details:** Starting Release 9.5, JUNOScope enables you to get the current interfaces details from the selected devices or device group, and update JUNOScope database with these details. To use this feature, go to the JUNOScope Sync Device Details wizard (Settings > Devices > Sync Device Details) and select the device (or group of devices) that you want to synchronize with the JUNOScope database.

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

- **Enhancement of JUNOScope functionality to support the updating of interface details for a device:** Starting Release 9.5, JUNOScope enables you to update the JUNOScope database with the details of a specific interface of a device. You can also provide a loopback address for the selected device. To use this feature, go to the JUNOScope Device page, select the device, and go to the JUNOScope Update Interface Details wizard (Settings > Devices > Update Interface Details).

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

Current Software Release

The current JUNOScope software release is Release 9.5R4. For information about installing the software release, see “Installing the JUNOScope Software” on page 11.

Outstanding Issue

The following issue is outstanding in the current JUNOScope release:

- When you deploy a script to both Routing Engines, the file is copied to the device and cannot be overwritten unless you have root permissions. The file copy action fails when you try to deploy the same script to either RE. This is because an existing file cannot be overwritten if you only have user permissions. (PR 443586)
- The JUNOS Software Upgrade process is initiated 22 minutes after you use the JUNOScript remote procedure call. (PR 446932)

JUNOScope Software Usage Guidelines

- Install Latest Appropriate Operating System Patches on page 6
- Verify the JUNOScope Image Against Values Published on the Juniper Networks Web Site on page 6
- Upgrading JUNOScope and Password Policies on page 6
- Protecting JUNOScope Data Files on page 6
- Always Use Strong Passwords on page 6
- Change the Default Install Time User from ‘admin’ to Another Name on page 7
- Disable Access to the Inventory Management System SQL Interface on page 8

- Do Not Enable Debugging on JUNOScope at Installation on page 8
- Use Only HTTPS to Connect from a Browser Client to the JUNOScope Server on page 8
- Use Only SSL to Connect from the JUNOScope Software to Network Devices on page 8
- Do Not Export JUNOScope Data in Clear Text or with the Encryption Key in the Exported Data on page 8
- Disable User Accounts After Login Failure Attempts Within The Time Window Are Exceeded on page 9
- Regularly Back Up the JUNOScope Software Server on page 9

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-9.5R4-sunos5.sh` for Solaris.

To generate the hash value, use the following command:

```
hostname% openssl dgst9.5R4-openssl dgst jtk-install-9.5R4-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 9
- Red Hat Enterprise Linux ES File Package Requirements on page 10
- JUNOScope Client Workstation Requirements on page 11
- RADIUS Server Requirements on page 11
- Syslog Server Requirements on page 11
- Installing the JUNOScope Software on page 11
- Reconfiguring the JUNOScope Software on page 12
- Reinstalling or Upgrading the JUNOScope Software on page 13
- Uninstalling the JUNOScope Software on page 13

System Requirements

The JUNOScope software runs on both Sun Solaris servers (see Table 1 on page 10) and Red Hat Linux servers (see Table 2 on page 10). 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 10 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 10 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 10). 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

Table 3: Red Hat Enterprise Linux ES File Package Requirements (continued)

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 12

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-9.5R4.X-sunos5-sparc.sh  
install-directory
```

or

```
hostname% download-directory/jtk-install-9.5R4.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-9.5R4.X-sunos5-sparc.sh` or `jtk-install-9.5R4.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 12.

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 13 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 18 lists the books included in the *Network Operations Guide* series. Table 6 on page 18 lists the manuals and release notes supporting JUNOS Software for J-series and SRX-series platforms. All documents are available at <http://www.juniper.net/techpubs/>.

Table 7 on page 20 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	

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

Book	Description
<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>Broadband Subscriber Management Solutions</i>	Describes residential subscriber management and how you can deploy solutions that include multisubscriber IP address assignment, service provisioning, authentication, authorization, accounting, and dynamic request services in your network
<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.
<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 Layer 2 Configuration Guide</i>	Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the <i>JUNOS Routing Protocols Configuration Guide</i> .
<i>MX-series Layer 2 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).

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

Book	Description
<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 instances, and unicast routing protocols.
<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>Subscriber Access</i>	Provides an overview of the subscriber access features of the JUNOS Software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods.
<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	

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

Book	Description
<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	
<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	

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

Book	Description
<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.
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-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 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.
<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 Software, 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 for J-series Services Routers and SRX-series Services Gateways Documentation

Book	Description
J-series and SRX-series Platforms	
<i>JUNOS Software 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 Software 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 Software for J-series Services Routers and SRX-series Services Gateways Documentation (continued)

Book	Description
<i>JUNOS Software 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 Software 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 Software, including JUNOS Software 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 Software.
J-series Only	
<i>JUNOS Software 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 Software.
<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 Software Migration Guide</i>	Provides instructions for migrating an SSG device running ScreenOS software to JUNOS Software or upgrading a J-series device to a later version of the JUNOS Software.
<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 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.
<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/customers/support/downloads/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

27 March 2009 —Revision 1, JUNOScope Release 9.5R1

6 July 2009 —Revision 2, JUNOScope Release 9.5R2

30 October 2009 —Revision 3, JUNOScope Release 9.5R3

19 February 2010—Revision 4, JUNOScope Release 9.5R4

Copyright © 2010, 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.