Junos® OS

J-Web User Guide for Security Devices

Modified: 2018-03-23

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS J-Web User Guide for Security Devices

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- vSRX
- SRX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** *metric***>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(***string1* **|** *string2* **|** *string3***)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 Partner Support Service support contract, or are covered under warranty, and need post-sales 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

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 https://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, see https://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Understanding the J-Web User Interface

J-Web Overview

The J-Web interface allows you to monitor, configure, troubleshoot, and manage the routing platform by means of a Web browser enabled with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). J-Web provides access to all the configuration statements supported by the routing platform, so you can fully configure it without using the Junos OS CLI.

You can perform the following tasks with the J-Web interface:

- Monitoring—Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.
- Configuring—The J-Web interface provides the following different configuration methods:
  - Configure the routing platform quickly and easily without configuring each statement individually.
  - Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.
  - Edit the configuration in a text file.
  - Upload a configuration file.

  The J-Web interface also allows you to manage configuration history and set a rescue configuration.
- Troubleshooting—Troubleshoot routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze routing platform control traffic.

- Maintaining—Manage log, temporary, and core (crash) files and schedule reboots on the routing platforms.
- Configuring and monitoring events—Filter and view system log messages that record events occurring on the router. You can configure files to log system log messages and also assign attributes, such as severity levels, to messages.

Starting the J-Web User Interface

Before you start the user interface, you must perform the initial device configuration described in the Getting Started Guide for your device. After the initial configuration, you use your username and password, and the hostname or IP address of the device, to start the user interface.

To start the J-Web user interface:

1. Launch your HTTP-enabled or HTTPS-enabled Web browser.

   To use HTTPS, you must have installed the certificate provided by the device.

   NOTE: **If the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the device.**

2. Type **http://** or **https://** in your Web browser followed by the hostname or IP address of the device, and press Enter.

   The J-Web login page appears.

3. Type your username and password, and click **Log In**.

   To correct or change the username or password you typed, click **Reset**, type the new entry or entries, and click **Log In**.

   NOTE: **The default username is root with no password. You must change this during initial configuration or the system does not accept the configuration.**

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

Understanding the J-Web Interface Layout

Each page of the J-Web interface is divided into the following panes, as shown in Figure 1 on page 5.

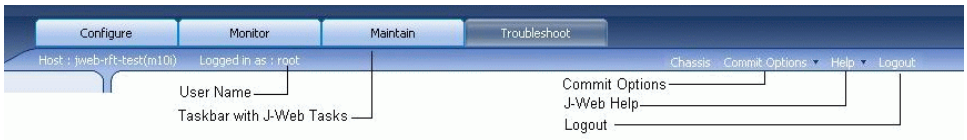
Figure 1: J-Web Layout

- Top pane—Displays identifying information and links.
- Main pane—Location where you monitor, configure, troubleshoot, and manage the Juniper Networks device by entering information in text boxes, making selections, and clicking buttons.
- Side pane—Displays subtasks of the Configure, Monitor, Maintain, or Troubleshoot task currently displayed in the main pane. For the configuration editor, this pane displays the hierarchy of configuration statements committed on the router. Click an item to access it in the main pane.

Top Pane

The top pane comprises the elements shown in Figure 2 on page 5.

Figure 2: Top Pane Elements



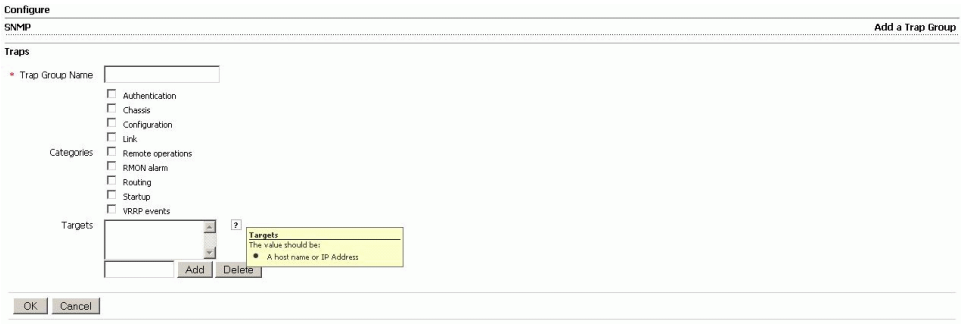
- *hostname – model*—Hostname and model of the Juniper Networks device.
- Logged in as: *username*—Username you used to log in to the device.
- Chassis—The chassis view of the device.
- Commit Options
  - Commit—Commits the candidate configuration. Changes made by other users as well as changes made in other J-Web sessions will be committed.
  - Compare—Displays the differences between the committed and uncommitted configuration on the device.
  - Discard—Discards the candidate configuration. Changes made by other users as well as changes made in other J-Web sessions will be discarded.
  - Preference—Enables you to select preferences for committing configuration. **Commit Check** only validates the configuration and reports errors. **Commit** validates and commits the configuration specified on every J-Web page.
- Help
  - Help Contents—Link to context-sensitive help information.

    - About—Link to information about the J-Web interface, such as the version number.
- Logout—Ends your current login session with the Juniper Networks device and returns you to the login page.
- Taskbar—Menu of J-Web tasks. Click a J-Web task to access it.
    - **Configure**—Configure the device by using Configuration pages or the configuration editor, and view configuration history.
    - **Monitor**—View information about configuration and hardware on the device.
    - **Maintain**—Manage files and licenses, upgrade software, and reboot the device.
    - **Troubleshoot**—Troubleshoot network connectivity problems.

Main Pane

The main pane comprises the elements shown in Figure 3 on page 6.

Figure 3: Main Pane Elements

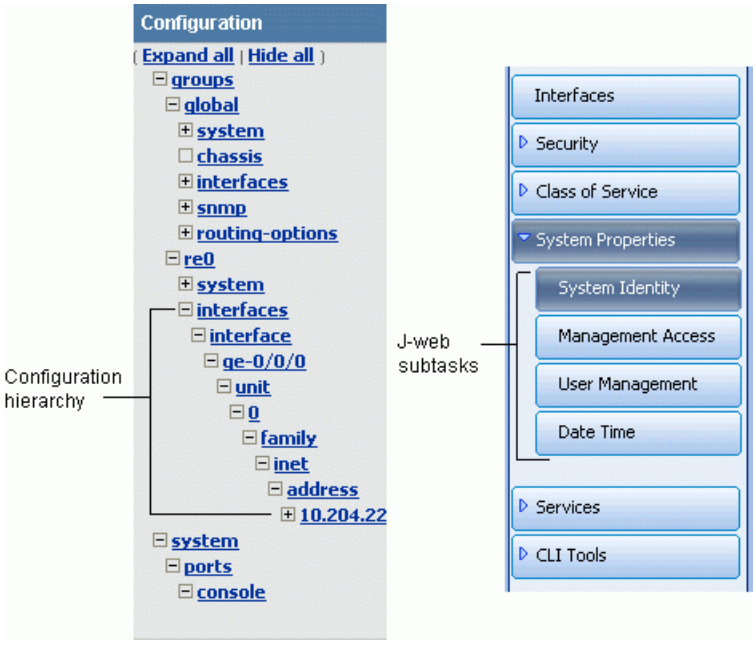


- Help (?) icon—Displays useful information when you move the cursor over the question mark. This help displays field-specific information, such as the definition, format, and valid range of the field.
- Red asterisk (*)—Indicates a required field.

Side Pane

The side pane comprises the elements shown in Figure 4 on page 7.

Figure 4: Side Pane Elements



- Subtask—Displays options related to the selected task in the J-Web taskbar.
- Configuration hierarchy—For the J-Web configuration editor, displays the hierarchy of committed statements in the device configuration.
  - Click **Expand all** to display the entire hierarchy.
  - Click **Hide all** to display only the statements at the top level.
  - Click plus signs (+) to expand individual items.
  - Click minus signs (–) to hide individual items.

Getting Help in the J-Web User Interface

To get Help in the J-Web user interface, use the following methods:

- Field-sensitive Help—Move the cursor over the question mark (**?**) next to the field for which you want more information. Typically, this Help includes one line of information about what this field does or what you must enter in a given text box. For example, Help for the Peer Autonomous System Number text box states, "The value should be a number between 1 and 65535."
- Context-sensitive Help—Click **Help** in the taskbar to open a separate page displaying the summary of all the fields on that page. To exit Help, close the page.
- Wizard Help (SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650)—Use the Firewall Policy, VPN, and NAT wizards to perform basic configurations. Click a field in a wizard page to display information about that field in the lower-left corner of the wizard page.

PART 2

Configuring and Managing a Device Using J-Web

CHAPTER 2

Installing J-Web

J-Web Software Requirements

To access the J-Web interface for all platforms, your management device requires the following software:

- Supported browsers— Microsoft Internet Explorer version 10 or 11, Mozilla Firefox version 44 or later, and Google Chrome version 55 or later; other browser versions might not provide access to J-Web

  NOTE: If you are accessing J-Web through a HTTPS protocol, the browser must be enabled with TLS version 1.2 and SSL version 3.0 or later.

- Language support— English-version browsers

Installing the J-Web Software

Your Juniper Networks device comes with the Junos OS installed on it. When you power on the Juniper device, all software starts automatically.

If your device is not shipped with the J-Web software on it, you must download the J-Web software package from the Juniper Networks webpage and install it on your device. After the installation, you must enable Web management of the device with the CLI.

To install and enable the J-Web software:

1. Using a Web browser, navigate to the Juniper Networks Customer Support Center at https://www.juniper.net/customers/csc/software/.

2. Log in to the Juniper Networks authentication system with the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Download the J-Web software to your local host. Select the version that is the same as the Junos OS version running on the device.

4. Copy the software package to the device. We recommend that you copy it to the **/var/tmp** directory.

5. If you have previously installed the J-Web software on the device, you must delete it before installing the new version. To do so, from operational mode in the CLI, enter the following command:

   user@host> **request system software delete jweb**

6. Install the new package on the device. From operational mode in the CLI, enter the following command:

   user@host> **request system software add *path/filename***

   Replace ***path*** with the full pathname to the J-Web software package. Replace ***filename*** with the filename of the J-Web software package.

7. Enable Web management of the device. From configuration mode in the CLI, enter the following command:

   user@host# **system services web-management http**

NOTE: On SRX340 and SRX345 devices, the factory-default configuration has a generic HTTP configuration. To use ge and fxp0 ports as management ports, you must use the **set system services web-management http** command. The Web management HTTP and HTTPS interfaces are changed to fxp0.0 and from ge-0/0/1.0 through ge-0/0/7.0

CHAPTER 3

Configuring Secure Web Access to a Device

Secure Web Access Overview

A Juniper Networks device uses the Secure Sockets Layer (SSL) protocol to provide secure management of devices through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the device through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you are not able to access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

Generating SSL Certificates

To enable secure Web access, you must first generate a digital SSL certificate, and then enable HTTPS access on the Juniper Networks device.

To generate an SSL certificate:

1. Enter the following **openssl** command in your Secure Shell command-line interface. The **openssl** command generates a self-signed SSL certificate in the Privacy-Enhanced Mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

NOTE: Run this command on a LINUX or UNIX device because Juniper Networks Services Gateways do not support the openssl command.

% openssl req –x509 –nodes –newkey rsa:1024 –keyout *filename*.pem -out *filename*.pem

Replace ***filename*** with the name of a file in which you want the SSL certificate to be written—for example, **new.pem**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.

3. Display the contents of the **new.pem** file.

   cat new.pem

   Copy the contents of this file for installing the SSL certificate.

Go on to "Configuring Secure Web Access" on page 14 to install the SSL certificate and enable HTTPS.

Configuring Secure Web Access

Navigate to the Management Access Configuration page by selecting **Configure>System Properties>Management Access**. Click **Edit** from the main pane to open the Edit Management Access page. On this page, you can enable HTTP and HTTPS access on interfaces for managing Services Routers through the Web interface. You can also install SSL certificates and enable JUNOScript over SSL with the Secure Access page.

For more information, see *Help Contents* of this J-Web page.

Establishing J-Web Sessions

You establish a J-Web session through an HTTP-enabled or HTTPS-enabled Web browser. The HTTPS protocol, which uses 128-bit encryption, is available only in domestic versions of the Junos OS. To use HTTPS, you must have installed the certificate provided by the device.

When you attempt to log in through the J-Web interface, the system authenticates your username with the same methods used for Telnet and SSH.

The device can support multiple J-Web sessions for a single user who logs in to each session. However, if a single user attempts to launch multiple J-Web *windows*—for example, by right-clicking a link to launch another instance of a Web browser—the session can have unpredictable results.

If the device does not detect any activity through the J-Web user interface for 15 minutes, the session times out and is terminated. You must log in again to begin a new session.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

Table 3 on page 15 shows the maximum number of concurrent J-Web sessions on SRX Series devices.

Table 3: Concurrent Web Sessions on SRX Series Devices

Device Type	Maximum Number of Users
SRX300, SRX320, SRX340, SRX345, SRX1500	7
SRX5400, SRX5600, SRX5800	1024

CHAPTER 4

Managing a Configuration Using J-Web

Configuring Basic Settings

Before you begin initial configuration, complete the following tasks:

- Install the Juniper Networks device in its permanent location, as described in the hardware installation guide or the Getting Started Guide for your device.
- Gather the following information:
  - Hostname for the router on the network
  - Domain that the router belongs to on the network
  - Password for the root user
  - Time zone where the router is located
  - IP address of a Network Time Protocol (NTP) server (if NTP is used to set the time on the router)
  - IP address of a Domain Name System (DNS) server
  - List of domains that can be appended to hostnames for DNS resolution
  - IP address of the default gateway
  - IP address to be used for the loopback interface
  - IP address of the built-in Ethernet interface that you will use for management purposes
- Collect the following equipment:
  - A management device, such as a laptop, with an Ethernet port
  - An Ethernet cable

To configure basic settings with J-Web Initial Configuration:

1. Enter information into the Initial Configuration Set Up page (see Figure 5 on page 19), as described in Table 4 on page 19.

2. Click **Apply** to apply the configuration.

Figure 5: J-Web Set Up Initial Configuration Page

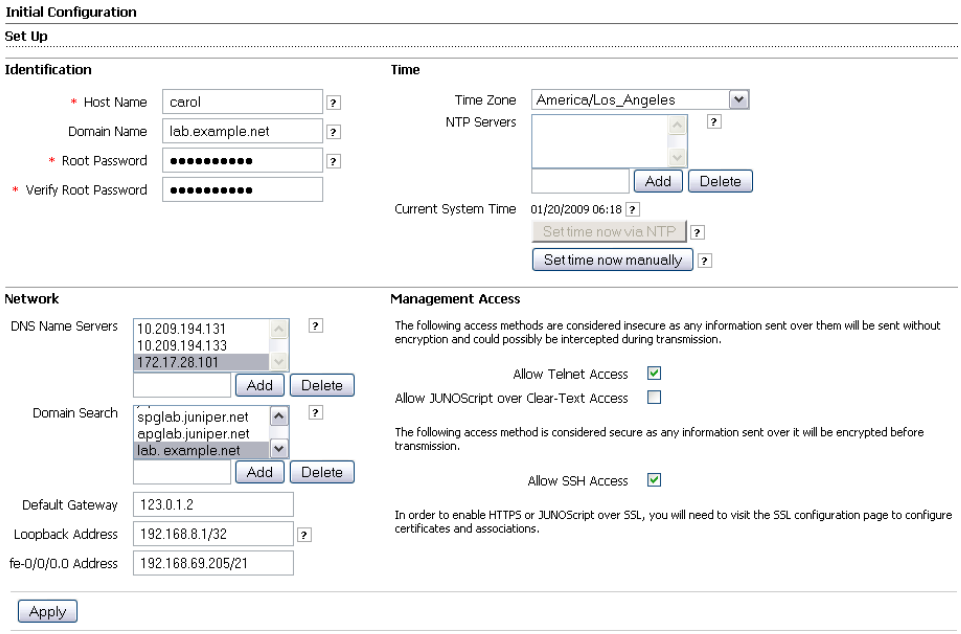


Table 4: Initial Configuration Set Up Summary

Field	Function	Your Action
Identification		
Host Name (required)	Defines the hostname of the router.	Type the hostname.
Domain Name	Defines the network or subnetwork that the machine belongs to.	Type the domain name.
Root Password (required)	Sets the root password that the user “root” can use to log in to the router.	Type a plain-text password that the system encrypts. NOTE: After a root password has been defined, it is required when you log in to the J-Web user interface or the CLI.
Verify Root Password (required)	Verifies that the root password has been typed correctly.	Retype the password.
Time		
Time Zone	Identifies the time zone that the router is located in.	From the list, select the appropriate time zone.
NTP Servers	Specify an NTP server that the router can reach to synchronize the system time.	To add an IP address, type it in the box to the left of the Add button, then click **Add**. To delete an IP address, click it in the box above the Add button, then click **Delete**.

Table 4: Initial Configuration Set Up Summary *(continued)*

Field	Function	Your Action
Current System Time	Synchronizes the system time with the NTP server, or manually sets the system time and date.	• To immediately set the time using the NTP server, click **Set Time via NTP**. The router sends a request to the NTP server and synchronizes the system time. NOTE: If you are configuring other settings on this page, the router also synchronizes the system time using the NTP server when you click **Apply**. • To set the time manually, click **Set Time Manually**. A pop-up window allows you to select the current date and time from lists.
Network		
DNS Name Servers	Specify a DNS server that the router can use to resolve hostnames into addresses.	To add an IP address, type it in the box to the left of the Add button, then click **Add**. To delete an IP address, click it in the box above the Add button, then click **Delete**.
Domain Search	Adds each domain name that the router is included in to the configuration so that they are included in a DNS search.	To add a domain name, type it in the box to the left of the Add button, then click **Add**. To delete a domain name, click it in the box above the Add button, then click **Delete**.
Default Gateway	Defines a default gateway through which to direct packets addressed to networks not explicitly listed in the routing table.	Type a 32-bit IP address, in dotted decimal notation.
Loopback Address	Defines a reserved IP address that is always available on the router. If no address is entered, this address is set to **127.0.0.1/32**.	Type a 32-bit IP address and prefix length, in dotted decimal notation.
Management Access		
Allow Telnet Access	Allows remote access to the router by using Telnet.	To enable Telnet access, select the check box.
Allow JUNOScript protocol over Clear-Text Access	Allows JUNOScript to access the router by using a protocol for sending unencrypted text over a TCP connection.	To enable JUNOScript access over clear text, select the check box.
Allow SSH Access	Allows remote access to the router by using SSH.	To enable SSH access, select the check box.

J-Web Configuration Pages Overview

J-Web configuration pages offer you several different ways to configure your Juniper Networks device. Configuration pages provide access to all the configuration statements

supported by the device, so you can fully configure it without using the CLI. You can also manage the configuration, monitor user access, and set a rescue configuration.

Table 5 on page 21 provides a summary of the J-Web configuration pages.

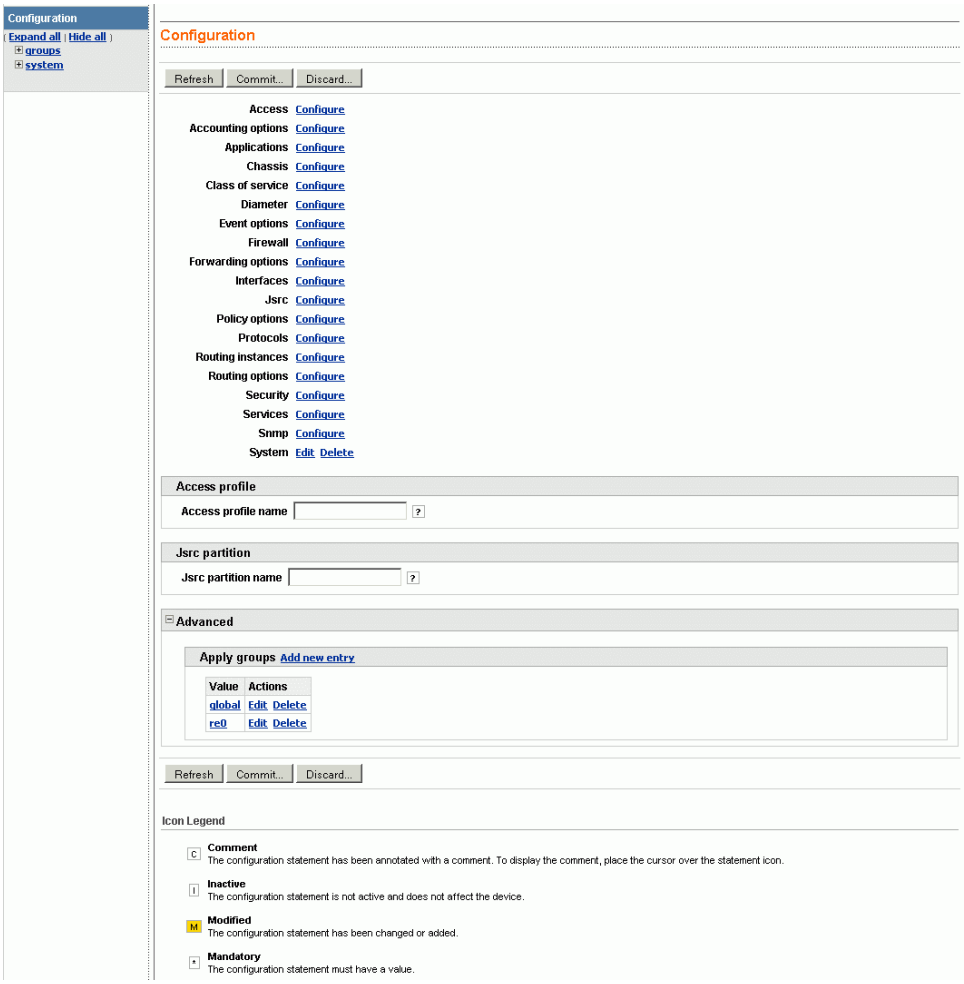
Table 5: J-Web Configuration Pages Summary

J-Web Configuration Task	Description	More Information
Edit the configuration using a clickable interface	Expand the entire configuration hierarchy in the side pane and click a configuration statement to view or edit. The main pane displays all the options for the statement, with a text box for each option.	For more information, go to **Configure>CLI Tools>Point and Click CLI** in the J-Web user interface.
Edit the configuration in text format	Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines in the configuration text.	For more information, go to **Configure>CLI Tools>CLI Editor** in the J-Web user interface.
Upload a configuration file	Upload a complete configuration.	For more information, go to **Maintain>Config Management>Upload** in the J-Web user interface.
View the configuration in text format	View the entire configuration on the device in text format.	For more information, go to **Configure>CLI Tools>CLI Viewer** in the J-Web user interface.

Editing a Configuration

To edit the configuration on a series of pages of clickable options that step you through the hierarchy, select **Configure>CLI Tools>Point and Click**. The side pane displays the top level of the configuration hierarchy, and the main pane displays configured hierarchy options and the Icon Legend (see Figure 6 on page 22).

Figure 6: Edit Configuration Page



See the video for an example of how to use the J-Web configuration editor to configure and manage stateless firewall filters.

Video: Managing Firewall Filters with J-Web

To expand or hide the hierarchy of all the statements in the side pane, click **Expand all** or **Hide all**. To expand or hide an individual statement in the hierarchy, click the expand (**+**) or collapse (**–**) icon to the left of the statement.

NOTE: **Only those statements included in the committed configuration are displayed in the side pane hierarchy.**

The configuration information in the main pane consists of configuration options that correspond to configuration statements. Configuration options that contain subordinate statements are identified by the term *nested configuration*.

To include, edit, or delete statements in the candidate configuration, click one of the links described in Table 6 on page 23 in the main pane. Then specify configuration information by typing into a field, selecting a value from a list, or clicking a check box (toggle).

Table 6: J-Web Edit Configuration Links

Link	Function
Add new entry	Displays fields and lists for a statement identifier, allowing you to add a new identifier to a statement.
Configure	Displays information for a configuration option that has not been configured, allowing you to include a statement.
Delete	Deletes the corresponding statement or identifier from the configuration. All subordinate statements and identifiers contained within a deleted statement are also discarded.
Edit	Displays information for a configuration option that has already been configured, allowing you to edit a statement.
identifier	Displays fields and lists for an existing statement identifier, allowing you to edit the identifier.

As you navigate through the configuration, the hierarchy level is displayed at the upper right of the main pane. You can click a statement or identifier in the hierarchy to return to the corresponding configuration options in the main pane.

The main pane includes icons that display information about statements and identifiers when you place your cursor over them. Table 7 on page 23 describes the meaning of these icons.

Table 7: J-Web Edit Configuration Icons

Icon	Meaning
C	Displays a comment about a statement.
I	Indicates that a statement is inactive.
M	Indicates that a statement has been added or modified, but has not been committed.
*	Indicates that the statement or identifier is required in the configuration.
?	Provides Help information.

J-Web Commit Options Guidelines

Using the J-Web Commit Preference, you can configure the commit options either to commit all global configurations together or to commit each configuration change immediately. Do one of the following to commit a configuration:

- Set Commit Preference to **Validate and commit configuration changes**, and then click **OK**.
- Set Commit Preference to **Validate configuration changes**, click **OK** to check your configuration and save it as a candidate configuration, and then click **Commit Options**>**Commit**.

For example, suppose you want to delete a firewall and add a new one.

- If Commit Preference is set to **Validate and commit configuration changes**, then you would need to commit your changes twice for each action.
- If Commit Preference is set to **Validate configuration changes**, then you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, allowing other users to edit those configurations, but the changes do not take effect on the device platform until you commit them. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration when you commit the candidate configuration, changes made by all the users take effect.

You use the single commit feature to commit all your configurations in J-Web simultaneously. This helps to reduce the time J-Web takes to commit configurations because when changes are committed at every step, rollback configurations pile up quickly.

NOTE: If you end a session with a particular Commit Preference, the subsequent sessions for that particular browser will automatically come up with the preference you previously selected. If you start the subsequent session on a different browser, the session will come up with the default commit preference.

NOTE: There are some pages whose configurations would need to be committed immediately. For such pages, even if you configure the commit options to perform a single global commit for them, the system displays appropriate information notification windows to remind you to commit your changes immediately. Examples of such pages are Switching, Interfaces, and Class of Service.

Committing a Configuration

When you finish making changes to a candidate configuration with the J-Web configuration editor, you must commit the changes to use them in the current operational software running on the Juniper Networks device.

If another user is editing an exclusive candidate configuration with the CLI, you cannot commit a configuration until the user has committed the configuration. For more information about editing an exclusive candidate configuration, see the *Junos OS CLI User Guide*.

To commit a candidate configuration:

1. In the J-Web configuration editor, click **Commit**.

   The main pane displays a summary of your changes in statement form.

2. To confirm the commit operation, click **OK**.

   If multiple users are editing the configuration when you commit the candidate configuration, all changes made by all users take effect.

3. To display all the edits applied to the running configuration, click **Refresh**.

CHAPTER 5

Managing J-Web Sessions and Users

Setting J-Web Session Limits

By default, an unlimited number of users can log in to the J-Web interface on a Juniper Networks device, and each session remains open for 24 hours (1440 minutes). Using CLI commands, you can limit the maximum number of simultaneous J-Web user sessions and set a default session timeout for all users.

- To limit the number of simultaneous J-Web user sessions, enter the following commands:

  user@host# **edit system services web-management session**
  user@host# **set session-limit** ***session-limit***

  Range: **1** through **1024**. Default: Unlimited

- To change the J-Web session idle time limit, enter the following commands:

  user@host# **edit system services web-management session**
  user@host# **set idle-timeout** ***minutes***

  Range: **1** through **1440**. Default: **1440**

You can also configure the maximum number of simultaneous subordinate HTTP processes that the device creates in response to user requests.

To configure the maximum number of subordinate httpd processes, enter the following commands:

user@host# **edit system services web-management limits**

user@host# **active-child-process** ***process-limit***

The default is **5**, and the range is **0** through **32**.

Terminating J-Web Sessions

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane. You must log in again to begin a new session.

By default, if the Juniper Networks device does not detect any activity through the J-Web interface for 24 hours, the session times out and is terminated. For information about changing the idle time limit, see "Setting J-Web Session Limits" on page 27.

CHAPTER 6

Monitoring and Managing a Device using J-Web

J-Web Packet Capture Results and Output Summary

Table 8 on page 29 summarizes the output in the packet capture display.

Table 8: J-Web Packet Capture Results and Output Summary

Field	Description
timestamp	Time when the packet was captured. The timestamp **00:45:40.823971** means 00 hours (12.00 a.m.), 45 minutes, and 40.823971 seconds. NOTE: The time displayed is local time.
direction	Direction of the packet. Specifies whether the packet originated from the Routing Engine (**Out**), or was destined for the Routing Engine (**In**).
protocol	Protocol for the packet. In the sample output, **IP** indicates the Layer 3 protocol.

Table 8: J-Web Packet Capture Results and Output Summary *(continued)*

Field	Description
source address	Hostname, if available, or IP address and the port number of the packet's origin. If the Don't Resolve Addresses check box is selected, only the IP address of the source displays. NOTE: When a string is defined for the port, the packet capture output displays the string instead of the port number.
destination address	Hostname, if available, or IP address of the packet's destination with the port number. If the Don't Resolve Addresses check box is selected, only the IP address of the destination and the port appear. NOTE: When a string is defined for the port, the packet capture output displays the string instead of the port number.
protocol	Protocol for the packet. In the sample output, **TCP** indicates the Layer 4 protocol.
data size	Size of the packet (in bytes).

Related Documentation

- *Packet Capture Overview*
- *Diagnostic Tools Overview*
- Using the J-Web Packet Capture Tool on page 36

J-Web Ping Host Results and Output Summary

Table 9 on page 30 summarizes the output in the ping host display.

Table 9: Ping Host Results and Output

Ping Host Result	Description
bytes **bytes from** ***ip-address***	• ***bytes*** —Size of ping response packet, which is equal to the value you entered in the Packet Size box, plus 8. • ***ip-address***—IP address of destination host that sent the ping response packet.
icmp_seq=0 **icmp_seq=***number*	***number***—Sequence Number field of the ping response packet. You can use this value to match the ping response to the corresponding ping request.
ttl=*number*	***number***—Time-to-live hop-count value of the ping response packet.
number **packets transmitted**	***number***—Number of ping requests (probes) sent to host.
percentage **packet loss**	***percentage***—Number of ping responses divided by the number of ping requests, specified as a percentage.

Table 9: Ping Host Results and Output *(continued)*

Ping Host Result	Description
round-trip min/avg/max/stddev = *min-time/avg-time/max-time/std-dev* ms	• ***min-time***—Minimum round-trip time (see **time=*time*** field in this table). • ***avg-time***—Average round-trip time. • ***max-time***—Maximum round-trip time. • ***std-dev***—Standard deviation of the round-trip times.

If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host might be configured to ignore ICMP echo requests.
- The host might be configured with a firewall filter that blocks ICMP echo requests or ICMP echo responses.
- The size of the ICMP echo request packet exceeds the MTU of a host along the path.
- The value you selected in the Time-to-Live box was less than the number of hops in the path to the host, in which case the host might reply with an ICMP error message.

Related Documentation

- *Diagnostic Tools Overview*
- *Understanding Ping MPLS*
- Using the J-Web Ping Host Tool on page 39
- *Interfaces Feature Guide for Security Devices*

J-Web Ping MPLS Results and Output Summary

Table 10 on page 31 summarizes the output in the ping MPLS display.

Table 10: J-Web Ping MPLS Results and Output Summary

Field	Description
Exclamation point (!)	Echo reply was received.
Period (.)	Echo reply was not received within the timeout period.
x	Echo reply was received with an error code. Errored packets are not counted in the received packets count and are accounted for separately.
number **packets transmitted**	***number***—Number of ping requests (probes) sent to a host.
number **packets received**	***number***—Number of ping responses received from a host.

Table 10: J-Web Ping MPLS Results and Output Summary *(continued)*

Field	Description
***percentage* packet loss**	***percentage***—Number of ping responses divided by the number of ping requests, specified as a percentage.
time	For Layer 2 circuits only, the number of milliseconds required for the ping packet to reach the destination. This value is approximate, because the packet has to reach the Routing Engine.

If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host might be configured to ignore echo requests.
- The host might be configured with a firewall filter that blocks echo requests or echo responses.
- The size of the echo request packet exceeds the MTU of a host along the path.
- The outbound node at the remote endpoint is not configured to handle MPLS packets.
- The remote endpoint's loopback address is not configured to **127.0.0.1**.

Related Documentation

- *Diagnostic Tools Overview*
- *Understanding Ping MPLS*
- Using the J-Web Ping MPLS Tool on page 41
- *Interfaces Feature Guide for Security Devices*

J-Web Traceroute Results and Output Summary

Table 11 on page 32 summarizes the output in the traceroute display.

Table 11: J-Web Traceroute Results and Output Summary

Field	Description
hop-number	Number of the hop (device) along the path.
host	Hostname, if available, or IP address of the device. If the Don't Resolve Addresses check box is selected, the hostname does not appear.
ip-address	IP address of the device.
as-number	AS number of the device.

Table 11: J-Web Traceroute Results and Output Summary *(continued)*

Field	Description
time1	Round-trip time between the sending of the first traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.
time2	Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.
time3	Round-trip time between the sending of the third traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.

If the device does not display the complete path to the destination host, one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host, or a router along the path, might be configured to ignore ICMP traceroute messages.
- The host, or a device along the path, might be configured with a firewall filter that blocks ICMP traceroute requests or ICMP time exceeded responses.
- The value you selected in the Time Exceeded box was less than the number of hops in the path to the host. In this case, the host might reply with an ICMP error message.

Related Documentation

- *Diagnostic Tools Overview*
- Using the J-Web Traceroute Tool on page 44

Monitoring Hosts Using the J-Web Ping Host Tool

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the J-Web ping host tool to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The switch sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

Action

To use the J-Web ping host tool:

1. Select **Troubleshoot>Ping Host**.
2. Next to Advanced options, click the expand icon.

3. Enter information into the Ping Host page, as described in Table 12 on page 34.

   The Remote Host field is the only required field.

4. Click **Start**.

   The results of the ping operation are displayed in the main pane . If no options are specified, each ping response is in the following format:

   ```
   bytes bytes from ip-address: icmp_seq=number ttl=number time=time
   ```

5. To stop the ping operation before it is complete, click **OK**.

Meaning Table 12 on page 34 lists the fields.

Table 12: J-Web Ping Host Field Summary

Field	Function	Your Action
Remote Host	Identifies the host to ping.	Type the hostname or IP address of the host to ping.
Advanced Options		
Don't Resolve Addresses	Determines whether to display hostnames of the hops along the path.	• To suppress the display of the hop hostnames, select the check box. • To display the hop hostnames, clear the check box.
Interface	Specifies the interface on which the ping requests are sent.	Select the interface on which ping requests are sent from the list. If you select **any**, the ping requests are sent on all interfaces.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list.
Don't Fragment	Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet.	• To set the DF bit, select the check box. • To clear the DF bit, clear the check box.
Record Route	Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane.	• To record and display the path of the packet, select the check box. • To suppress the recording and display of the path of the packet, clear the check box.
Type-of-Service	Specifies the type-of-service (TOS) value in the IP header of the ping request packet.	Select the decimal value of the TOS field from the list.
Routing Instance	Name of the routing instance for the ping attempt.	Select the routing instance name from the list.
Interval	Specifies the interval, in seconds, between transmissions of individual ping requests.	Select the interval from the list.
Packet Size	Specifies the size of the ping request packet.	Type the size, in bytes, of the packet. The size can be from 0 through 65468. The switch adds 8 bytes of ICMP header to the size.

Table 12: J-Web Ping Host Field Summary *(continued)*

Field	Function	Your Action
Source Address	Specifies the source address of the ping request packet.	Type the source IP address.
Time-to-Live	Specifies the time-to-live (TTL) hop count for the ping request packet.	Select the TTL value from the list.
Bypass Routing	Determines whether ping requests are routed by means of the routing table. If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.	• To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box. • To route the ping requests using the routing table, clear the check box.

Related Documentation

- *Monitoring Interface Status and Traffic*

Monitoring System Log Messages with the J-Web Event Viewer

Purpose Monitor errors and events that occur on the device.

Action Select **Monitor>Events and Alarms>View Events** in the J-Web user interface.

The J-Web View Events page displays the following information about each event:

- Process—System process that generated the error or event.
- Severity— A severity level indicates how seriously the triggering event affects routing platform functions. Only messages from the facility that are rated at that level or higher are logged. Possible severities and their corresponding color code are:
  - Debug/Info/Notice (Green)—Indicates conditions that are not errors but are of interest or might warrant special handling.
  - Warning (Yellow)—Indicates conditions that warrant monitoring.
  - Error (Blue)—Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
  - Critical (Pink)—Indicates critical conditions, such as hard drive errors.
  - Alert (Orange)—Indicates conditions that require immediate correction, such as a corrupted system database.
  - Emergency (Red)—Indicates system panic or other conditions that cause the routing platform to stop functioning.
- Event ID—Unique ID of the error or event. The prefix on each code identifies the generating software process. The rest of the code indicates the specific event or error.

- Event Description—Displays a more detailed explanation of the message.
- Time—Time that the error or event occurred.

To control which errors and events are displayed in the list, use the following options:

- System Log File—Specify the name of the system log file that records the errors and events.
- Process—Specify the system processes that generate the events you want to display. To view all the processes running on your system, enter the **show system processes** CLI command.
- Date From—Specify the beginning of the date range that you want to monitor. Set the date using the calendar pick tool.
- To—Specify the end of the date range that you want to monitor. Set the date using the calendar pick tool.
- Event ID—Specify the specific ID of the error or event that you want to monitor.
- Description—Enter a description for the errors or events.
- Search—Fetches the errors and events specified in the search criteria.
- Reset—Clears the cache of errors and events that were previously selected.
- Generate Report—Creates an HTML report based on the specified parameters.

Related Documentation

- *Understanding System Logging for Security Devices*
- *Understanding Binary Format for Security Logs*
- *Monitoring Overview*
- *Monitoring Interfaces*

Using the J-Web Packet Capture Tool

You can use the J-Web packet capture diagnostic tool when you need to quickly capture and analyze router control traffic on a device. Packet capture on the J-Web user interface allows you to capture traffic destined for, or originating from, the Routing Engine. You can use the J-Web packet capture tool to compose expressions with various matching criteria to specify the packets that you want to capture. You can either choose to decode and view the captured packets in the J-Web user interface as they are captured, or save the captured packets to a file and analyze them offline using packet analyzers such as Ethereal. The J-Web packet capture tool does not capture transient traffic.

To capture transient traffic and entire IPv4 data packets for offline analysis, you must configure packet capture with the J-Web user interface or CLI configuration editor.

To use J-Web packet capture:

1. Select **Troubleshoot>Packet Capture**.

2. Enter information into the Packet Capture page (see Table 13 on page 37). The sample configuration captures the next 10 TCP packets originating from the IP address **10.1.40.48** on port 23 and passing through the Gigabit Ethernet interface **ge-0/0/0**.

3. Save the captured packets to a file, or specify other advanced options by clicking the expand icon next to Advanced options.

4. Click **Start**.

   The captured packet headers are decoded and appear in the Packet Capture display.

5. Do one of the following:

   - To stop capturing the packets and stay on the same page while the decoded packet headers are being displayed, click **Stop Capturing**.
   - To stop capturing packets and return to the Packet Capture page, click **OK**.

Table 13: Packet Capture Field Summary

Field	Function	Your Action
Interface	Specifies the interface on which the packets are captured. If you select **default**, packets on the Ethernet management port 0 are captured.	Select an interface from the list—for example, **ge-0/0/0**.
Detail level	Specifies the extent of details to be displayed for the packet headers. • Brief—Displays the minimum packet header information. This is the default. • Detail—Displays packet header information in moderate detail. • Extensive—Displays the maximum packet header information.	Select **Detail** from the list.
Packets	Specifies the number of packets to be captured. Values range from **1** to **1000**. Default is **10**. Packet capture stops capturing packets after this number is reached.	Select the number of packets to be captured from the list—for example, **10**.

Table 13: Packet Capture Field Summary *(continued)*

Field	Function	Your Action
Addresses	Specifies the addresses to be matched for capturing the packets using a combination of the following parameters: • Direction—Matches the packet headers for IP address, hostname, or network address of the source, destination or both. • Type—Specifies if packet headers are matched for host address or network address. You can add multiple entries to refine the match criteria for addresses.	Select address-matching criteria. For example: 1. From the Direction list, select **source**. 2. From the Type list, select **host**. 3. In the Address box, type **10.1.40.48**. 4. Click **Add**.
Protocols	Matches the protocol for which packets are captured. You can choose to capture TCP, UDP, or ICMP packets or a combination of TCP, UDP, and ICMP packets.	Select a protocol from the list—for example, **tcp**.
Ports	Matches packet headers containing the specified source or destination TCP or UDP port number or port name.	Select a direction and a port. For example: 1. From the Type list, select **src**. 2. In the Port box, type **23**.
Advanced Options		
Absolute TCP Sequence	Specifies that absolute TCP sequence numbers are to be displayed for the packet headers.	• Display absolute TCP sequence numbers in the packet headers by selecting this check box. • Stop displaying absolute TCP sequence numbers in the packet headers by clearing this check box.
Layer 2 Headers	Specifies that link-layer packet headers to display.	• Include link-layer packet headers while capturing packets, by selecting this check box. • Exclude link-layer packet headers while capturing packets by clearing this check box.
Non-Promiscuous	Specifies not to place the interface in promiscuous mode, so that the interface reads only packets addressed to it. In promiscuous mode, the interface reads every packet that reaches it.	• Read all packets that reach the interface by selecting this check box. • Read only packets addressed to the interface by clearing this check box.
Display Hex	Specifies that packet headers, except link-layer headers, are to be displayed in hexadecimal format.	• Display the packet headers in hexadecimal format by selecting this check box. • Stop displaying the packet headers in hexadecimal format by clearing this check box.
Display ASCII and Hex	Specifies that packet headers are to be displayed in hexadecimal and ASCII format.	• Display the packet headers in ASCII and hexadecimal formats by selecting this check box. • Stop displaying the packet headers in ASCII and hexadecimal formats by clearing this check box.

Table 13: Packet Capture Field Summary *(continued)*

Field	Function	Your Action
Header Expression	Specifies the match condition for the packets to capture. The match conditions you specify for Addresses, Protocols, and Ports appear in expression format in this field.	Enter match conditions in expression format or modify the expression composed from the match conditions you specified for Addresses, Protocols, and Ports. If you change the match conditions specified for Addresses, Protocols, and Ports again, packet capture overwrites your changes with the new match conditions.
Packet Size	Specifies the number of bytes to be displayed for each packet. If a packet header exceeds this size, the display is truncated for the packet header. The default value is 96 bytes.	Type the number of bytes you want to capture for each packet header—for example, **256**.
Don't Resolve Addresses	Specifies that IP addresses are not to be resolved into hostnames in the packet headers displayed.	• Prevent packet capture from resolving IP addresses to hostnames by selecting this check box. • Resolve IP addresses into hostnames by clearing this check box.
No Timestamp	Suppresses the display of packet header timestamps.	• Stop displaying timestamps in the captured packet headers by selecting this check box. • Display the timestamp in the captured packet headers by clearing this check box.
Write Packet Capture File	Writes the captured packets to a file in PCAP format in **/var/tmp**. The files are named with the prefix **jweb-pcap** and the extension **.pcap**. If you select this option, the decoded packet headers do not appear on the packet capture page.	• Save the captured packet headers to a file by selecting this check box. • Decode and display the packet headers on the J-Web page by clearing this check box.

Related Documentation

- *Packet Capture Overview*
- *Diagnostic Tools Overview*
- J-Web Packet Capture Results and Output Summary on page 29
- Using the J-Web Ping MPLS Tool on page 41
- Using the J-Web Ping Host Tool on page 39
- Using the J-Web Traceroute Tool on page 44

Using the J-Web Ping Host Tool

You can ping a host to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The device sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

Alternatively, you can use the CLI **ping** command. (See *Using the ping Command*.)

To use the ping host tool:

1. Select **Troubleshoot>Ping Host** from the task bar.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Ping Host page (see Table 14 on page 40).

Table 14: J-Web Ping Host Field Summary

Field	Function	Your Action
Remote Host	Identifies the host to ping. This is the only required field.	Type the hostname or IP address of the host to ping.
Advanced Options		
Don't Resolve Addresses	Determines whether to display hostnames of the hops along the path.	• Suppress the display of the hop hostnames by selecting the check box. • Display the hop hostnames by clearing the check box.
Interface	Specifies the interface on which the ping requests are sent.	Select the interface on which ping requests are sent from the list. If you select **any**, the ping requests are sent on all interfaces.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list.
Don't Fragment	Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet.	• Set the DF bit by selecting the check box. • Clear the DF bit by clearing the check box.
Record Route	Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane.	• Record and display the path of the packet by selecting the check box. • Suppress the recording and display of the path of the packet by clearing the check box.
Type-of-Service	Specifies the type-of-service (TOS) value in the IP header of the ping request packet.	Select the decimal value of the TOS field from the list.
Routing Instance	Names the routing instance for the ping attempt.	Select the routing instance name from the list.
Interval	Specifies the interval, in seconds, between the transmission of each ping request.	Select the interval from the list.
Packet Size	Specifies the size of the ping request packet.	Type the size, in bytes, of the packet. The size can be from 0 through 65,468. The device adds 8 bytes of ICMP header to the size.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address.
Time-to-Live	Specifies the time-to-live (TTL) hop count for the ping request packet.	Select the TTL from the list.

Table 14: J-Web Ping Host Field Summary *(continued)*

Field	Function	Your Action
Bypass Routing	Determines whether ping requests are routed by means of the routing table. If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.	• Bypass the routing table and send the ping requests to hosts on the specified interface only by selecting the check box. • Route the ping requests using the routing table by clearing the check box.

4. Click **Start**.

   The results of the ping operation appear in the main pane. If no options are specified, each ping response is in the following format:

   bytes bytes from *ip-address*: icmp_seq=*number* ttl=*number* time=*time*

5. You can stop the ping operation before it is complete by clicking **OK**.

Related Documentation

- *Diagnostic Tools Overview*
- *Understanding Ping MPLS*
- J-Web Ping Host Results and Output Summary on page 30
- Using the J-Web Traceroute Tool on page 44
- Using the J-Web Ping MPLS Tool on page 41
- Using the J-Web Packet Capture Tool on page 36

Using the J-Web Ping MPLS Tool

Before using the ping MPLS feature, make sure that the receiving interface on the VPN or LSP remote endpoint has MPLS enabled, and that the loopback interface on the outbound node is configured as **127.0.0.1**. The source address for MPLS probes must be a valid address on the device.

To use the ping MPLS tool:

1. Select **Troubleshoot>Ping MPLS** from the task bar.
2. Next to the ping MPLS option you want to use, click the expand icon.
3. Enter information into the Ping MPLS page (see Table 15 on page 42).

Table 15: J-Web Ping MPLS Field Summary

Field	Function	Your Action
Ping RSVP-signaled LSP		
LSP Name	Identifies the LSP to ping.	Type the name of the LSP to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a device interface.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping LDP-signaled LSP		
FEC Prefix	Identifies the LSP to ping.	Type the forwarding equivalence class (FEC) prefix and length of the LSP to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a device interface.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping LSP to Layer 3 VPN prefix		
Layer 3 VPN Name	Identifies the Layer 3 VPN to ping.	Type the name of the VPN to ping.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
VPN Prefix	Identifies the IP address prefix and length of the Layer 3 VPN to ping.	Type the IP address prefix and length of the VPN to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a device interface.
Locate LSP using interface name		
Interface	Specifies the interface on which the ping requests are sent.	Select the device interface on which ping requests are sent from the list. If you select **any**, the ping requests are sent on all interfaces.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a device interface.

Table 15: J-Web Ping MPLS Field Summary *(continued)*

Field	Function	Your Action
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Instance to which this connection belongs		
Layer 2VPN Name	Identifies the Layer 2 VPN to ping.	Type the name of the VPN to ping.
Remote Site Identifier	Specifies the remote site identifier of the Layer 2 VPN to ping.	Type the remote site identifier for the VPN.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a device interface.
Local Site Identifier	Specifies the local site identifier of the Layer 2 VPN to ping.	Type the local site identifier for the VPN.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Locate LSP from interface name		
Interface	Specifies the interface on which the ping requests are sent.	Select the device interface on which ping requests are sent from the list. If you select **any**, the ping requests are sent on all interfaces.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a device interface.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Locate LSP from virtual circuit information		
Remote Neighbor	Identifies the remote neighbor (PE device) within the virtual circuit to ping.	Type the IP address of the remote neighbor within the virtual circuit.
Circuit Identifier	Specifies the virtual circuit identifier for the Layer 2 circuit to ping.	Type the virtual circuit identifier for the Layer 2 circuit.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a device interface.

Table 15: J-Web Ping MPLS Field Summary *(continued)*

Field	Function	Your Action
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping end point of LSP		
VPN Prefix	Identifies the LSP endpoint to ping.	Type either the LDP FEC prefix and length or the RSVP LSP endpoint address for the LSP to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a device interface.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.

4. Click **Start**.

5. You can stop the ping operation before it is complete by clicking **OK**.

Related Documentation

- *Diagnostic Tools Overview*
- *Understanding Ping MPLS*
- J-Web Ping MPLS Results and Output Summary on page 31
- Using the J-Web Traceroute Tool on page 44
- Using the J-Web Ping Host Tool on page 39
- Using the J-Web Packet Capture Tool on page 36

Using the J-Web Traceroute Tool

You can use the traceroute diagnostic tool to display a list of devices between the device and a specified destination host. The output is useful for diagnosing a point of failure in the path from the device to the destination host, and addressing network traffic latency and throughput problems.

The device generates the list of devices by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive device is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner,

each device along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

To use the traceroute tool:

1. Select **Troubleshoot>Traceroute**.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Traceroute page (see Table 16 on page 45).

Table 16: Traceroute Field Summary

Field	Function	Your Action
Remote Host	Identifies the destination host of the traceroute. The **Remote Host** field is the only required field.	Type the hostname or IP address of the destination host.
Advanced Options		
Don't Resolve Addresses	Determines whether hostnames of the hops along the path are displayed, in addition to IP addresses.	• Suppress the display of the hop hostnames by selecting the check box. • Display the hop hostnames by clearing the check box.
Gateway	Specifies the IP address of the gateway to route through.	Type the gateway IP address.
Source Address	Specifies the source address of the outgoing traceroute packets.	Type the source IP address.
Bypass Routing	Determines whether traceroute packets are routed by means of the routing table. If the routing table is not used, traceroute packets are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, traceroute responses are not sent.	• Bypass the routing table and send the traceroute packets to hosts on the specified interface only by selecting the check box. • Route the traceroute packets by means of the routing table bu clearing the check box.
Interface	Specifies the interface on which the traceroute packets are sent.	Select the interface on which traceroute packets are sent from the list. If you select **any**, the traceroute requests are sent on all interfaces.
Time-to-Live	Specifies the maximum time-to-live (TTL) hop count for the traceroute request packet.	Select the TTL from the list.
Type-of-Service	Specifies the type-of-service (TOS) value to include in the IP header of the traceroute request packet.	Select the decimal value of the TOS field from the list.
Resolve AS Numbers	Determines whether the autonomous system (AS) number of each intermediate hop between the device and the destination host is displayed.	• Display the AS numbers by selecting the check box. • Suppress the display of the AS numbers by clearing the check box.

4. Click **Start**.

   The results of the traceroute operation are displayed in the main pane. If no options are specified, each line of the traceroute display is in the following format:

   hop-number host (*ip-address*) [*as-number*]*time1 time2 time3*

   The device sends a total of three traceroute packets to each router along the path and the round-trip time for each traceroute operation appears. If the device times out before receiving a **Time Exceeded** message, an asterisk (*) appears for that round-trip time.

5. You can stop the traceroute operation before it is complete by clicking **OK** while the results of the traceroute operation appear.

Related Documentation

- *Diagnostic Tools Overview*
- J-Web Traceroute Results and Output Summary on page 32
- Using the J-Web Ping MPLS Tool on page 41
- Using the J-Web Ping Host Tool on page 39
- Using the J-Web Packet Capture Tool on page 36

CHAPTER 7

Managing Files and Backup using J-Web

File Management Overview

You can use the J-Web user interface and the CLI to perform routine file management operations such as archiving log files and deleting unused log files, cleaning up temporary files and crash files, and downloading log files from the routing platform to your computer. You can also encrypt the configuration files with the CLI to prevent unauthorized users from viewing sensitive configuration information.

Before you perform any file management tasks, you must perform the initial device configuration described in the Getting Started Guide for your device.

Related Documentation

- Cleaning Up Files in J-Web on page 47
- *Cleaning Up Files with the CLI*
- *Managing Accounting Files*
- *Encrypting Configuration Files*
- *Decrypting Configuration Files*

Cleaning Up Files in J-Web

You can use the J-Web user interface to rotate log files and delete unnecessary files on the device. If you are running low on storage space, the file cleanup procedure quickly identifies files that can be deleted.

The file cleanup procedure performs the following tasks:

- Rotates log files—Archives all information in the current log files and creates fresh log files.
- Deletes log files in **/var/log**—Deletes any files that are not currently being written to.
- Deletes temporary files in **/var/tmp**—Deletes any files that have not been accessed within two days.
- Deletes all crash files in **/var/crash**—Deletes any core files that the device has written during an error.
- Deletes all software images (***.tgz** files) in **/var/sw/pkg**—Deletes any software images copied to this directory during software upgrades.

To rotate log files and delete unnecessary files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.
2. In the Clean Up Files section, click **Clean Up Files**. The device rotates log files and identifies the files that can be safely deleted.

   The J-Web user interface displays the files that you can delete and the amount of space that will be freed on the file system.
3. Click one of the following buttons on the confirmation page:
   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

Related Documentation

- *Managing Accounting Files*
- *Encrypting Configuration Files*
- *Decrypting Configuration Files*
- *Cleaning Up Files with the CLI*

Downloading Files

You can use the J-Web user interface to download a copy of an individual file from the device. When you download a file, it is not deleted from the file system.

To download files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.
2. In the Download and Delete Files section, click one of the following file types:
   - **Log Files**—Lists the log files located in the **/var/log** directory on the device.
   - **Temporary Files**—Lists the temporary files located in the **/var/tmp** directory on the device.

- **Old Junos OS**—Lists the software images located in the (***.tgz** files) in the **/var/sw/pkg** directory on the device.
- **Crash (Core) Files**—Lists the core files located in the **/var/crash** directory on the device.

  The J-Web user interface displays the files located in the directory.

3. Click **Download** to download an individual file.

4. Choose a location for the browser to save the file.

   The file is downloaded.

Related Documentation

- *Managing Accounting Files*

Deleting Files

You can use the J-Web user interface to delete an individual file from the device. When you delete the file, it is permanently removed from the file system.

CAUTION: **If you are unsure whether to delete a file from the device, we recommend using the Cleanup Files tool. This tool determines which files can be safely deleted from the file system.**

To delete files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.

2. In the Download and Delete Files section, click one of the following file types:
   - **Log Files**—Lists the log files located in the **/var/log** directory on the device.
   - **Temporary Files**—Lists the temporary files located in the **/var/tmp** directory on the device.
   - **Old Junos OS**—Lists the software images in the (***.tgz** files) in the **/var/sw/pkg** directory on the device.
   - **Crash (Core) Files**—Lists the core files located in the **/var/crash** directory on the device.

   The J-Web user interface displays the files located in the directory.

3. Check the box next to each file you plan to delete.

4. Click **Delete**.

The J-Web user interface displays the files you can delete and the amount of space that will be freed on the file system.

5. Click one of the following buttons on the confirmation page:
   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

Related Documentation
- *Managing Accounting Files*

Deleting the Backup Software Image

Junos OS keeps a backup image of the software that was previously installed so that you can downgrade to that version of the software if necessary. You can use the J-Web user interface to delete this backup image. If you delete this image, you cannot downgrade to this particular version of the software.

To delete the backup software image:

1. In the J-Web user interface, select **Maintain>Files**.
2. Review the backup image information listed in the Delete Backup Junos Package section.
3. Click the **Delete backup Junos package** link to delete the backup image.
4. Click one of the following buttons on the confirmation page:
   - To delete the backup image and return to the Files page, click **OK**.
   - To cancel the deletion of the backup image and return to the Files page, click **Cancel**.

Related Documentation
- Deleting Files on page 49

PART 3

Troubleshooting

CHAPTER 8

Troubleshooting the J-Web User Interface

Unpredictable J-Web Behavior

Problem **Description:** I have multiple J-Web windows open and am experiencing unpredictable results.

Solution Close the extra windows. The Juniper Networks device can support multiple J-Web sessions for a single user who logs in to each session. However, if a single user attempts to launch multiple J-Web windows —for example, by right-clicking a link to launch another instance of a Web browser—the session can have unpredictable results.

No J-Web Access

Problem **Description:** I cannot access J-Web from my browser.

Solution **Solution 1—**On the Juniper Networks device, verify that you have successfully installed the J-Web software package and enabled Web management on the platform, as described in "Installing the J-Web Software" on page 11.

Solution 2—If the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the **Use SSL 3.0** option in the Web browser to access J-Web on the device.