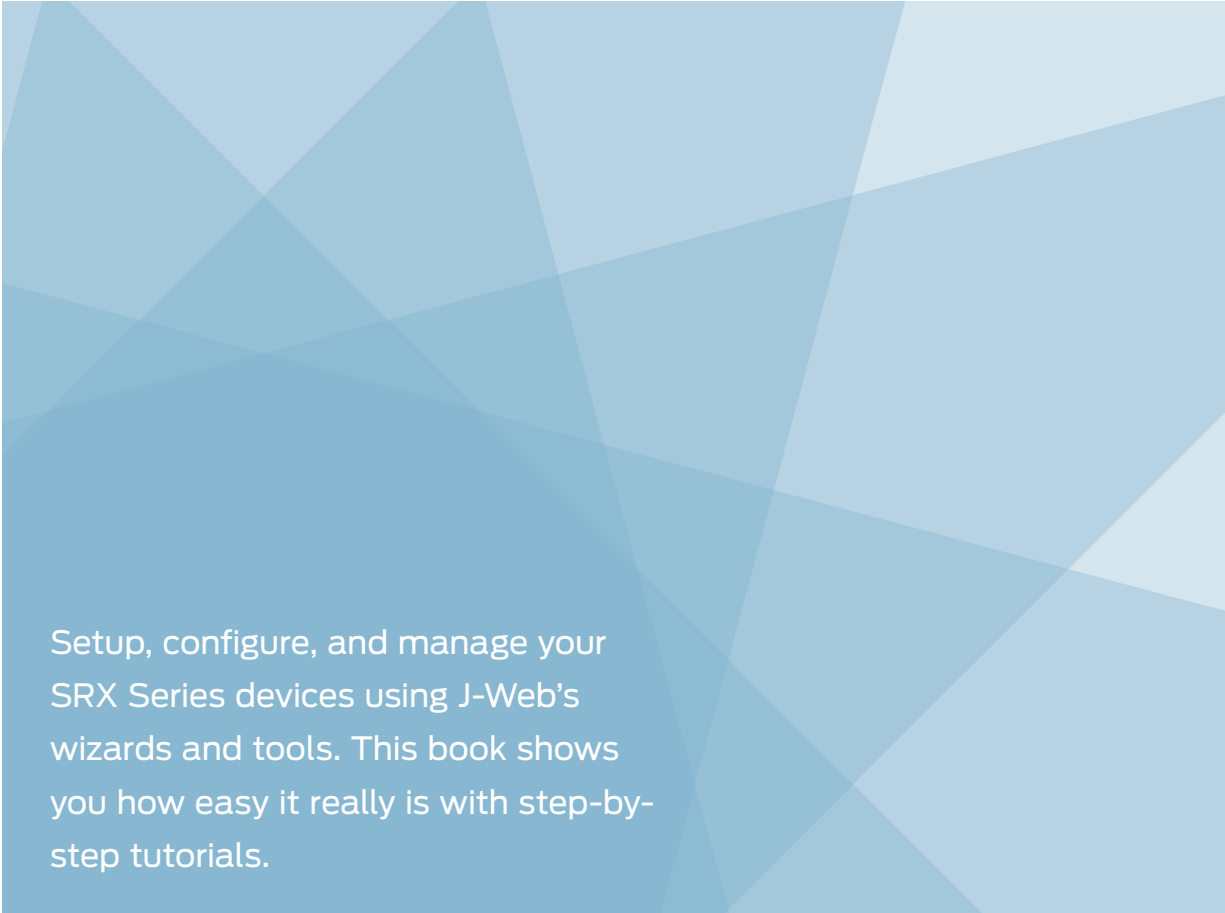


DAY ONE: CONFIGURING SRX SERIES WITH J-WEB



Setup, configure, and manage your SRX Series devices using J-Web's wizards and tools. This book shows you how easy it really is with step-by-step tutorials.

By Manekar Umamaheshwararao & Mark Smallwood

DAY ONE: CONFIGURING SRX SERIES WITH J-WEB

The SRX Series devices pack a diverse and powerful set of functionality into a small box that allows you to use it as a router, a firewall, for switching, and even as a DHCP server, client, or relay agent. J-Web ships with every SRX device providing a GUI management tool that brings context to all of the device interfaces, Junos protocols, security features, and services.

Yes, you could use the CLI to configure all of this functionality. And many administrators do. But this book shows you just how easy it can be to navigate the device with J-Web, and how J-Web helps you build a more complete mental image of your network. J-Web combines a modern interface along with a set of intuitive wizards that makes it especially easy to setup, configure, monitor, and maintain your device.

"This Day One book for configuring SRX Series with J-Web makes configuring, troubleshooting, and maintaining the SRX Series devices a breeze for any user who is new to the wonderful world of Junos, or who just likes to use its GUI interface rather than the CLI."

Alpana Nangpal, Security Engineer, Bravo Health

IT'S DAY ONE AND YOU HAVE A JOB TO DO, SO LEARN HOW TO:

- Access your SRX device using J-Web.
- Use the Initial Setup wizard to launch your SRX device for the first time.
- Use the other J-Web wizards to configure basic system properties like users, DNS, SNMP, DHCP and routing.
- Use J-Web to configure device security features like zones, screens, policies and NAT.
- Use J-Web to monitor network performance, upgrade software, and diagnose network problems.
- Explore the interface further, on your own, as the book guides you around your SRX device or test bed.

Juniper Networks Day One books provide just the information you need to know on day one. That's because they are written by subject matter experts who specialize in getting networks up and running. Visit www.juniper.net/dayone to peruse the complete library.

Published by Juniper Networks Books

ISBN 978-1-936779-12-3



9 781936 779123



7100 1333

JUNIPER
NETWORKS

Junos® Dynamic Services Series

Day One: Configuring SRX Series with J-Web

By Manekar Umamaheshwararao
and Mark Smallwood

<i>Chapter 1: Start Up, Connect, Log In.....</i>	<i>5</i>
<i>Chapter 2: Configuring the SRX with J-Web Wizards.....</i>	<i>23</i>
<i>Chapter 3: Configuring the SRX Device.....</i>	<i>33</i>
<i>Chapter 4: Configuring Device Security</i>	<i>49</i>
<i>Chapter 5: Monitoring with J-Web</i>	<i>65</i>
<i>Chapter 6: Diagnosing Network Problems</i>	<i>75</i>

© 2011 by Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. Junose 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.

Published by Juniper Networks Books

Writers: Manekar Umamaheshwararao and Mark Smallwood

Editor in Chief: Patrick Ames

Copyediting and Proofing: Nancy Koerbel

Junos Program Manager: Cathy Gadecki

ISBN: 978-1-936779-12-3 (print)

Printed in the USA by Vervante Corporation.

ISBN: 978-1-936779-13-0 (ebook)

Version History: v3 February 2011

2 3 4 5 6 7 8 9 10 #7100133-en

About the Authors

Manekar Umamaheshwararao (JNCIS-SEC, JNCIS-ER, JNCIA-EX) is a Sr. System Test Engineer with the SLT group at Juniper Networks, working on feature and performance testing for the High End and Branch Juniper security products (SRX Series Service Gateway). Prior to this role, Manekar worked as Technical Lead at Aricent and before that, he spent 4 years as R&D Engineer at Agilent developing software for Agilent N2X Multiservice Test Solution.

Mark Smallwood is a training specialist with the Engineering Training group at Juniper Networks, and managed the SRX publications team for its initial release.

Authors Acknowledgments

The authors want to thank their managers, Rajesh Patil, Manager, CSS-QA, and Gail Schilling, Director, Engineering Training, for their support of this project.

And a huge acknowledgment to Vairavan Subramanian for his careful and accurate technical review. Without it our tasks would seem endless.

This book is available in a variety of formats at: www.juniper.net/dayone.

Send your suggestions, comments, and critiques by email to dayone@juniper.net.

Follow the Day One series on Twitter: @Day1Junos

What You Need to Know Before Reading this Book

Before reading this book you should have a basic understanding of the Junos operating system. You may reference other Day One books and free online training to help you acquire this background.

Other knowledge that will be helpful to you as you read:

- ✓ A basic understanding of network devices and their settings is needed to fill in the fields of the J-Web configuration wizards.
- ✓ Basic technical knowledge and experience with networks, routing, and network security.
- ✓ It would be helpful to have *Day One: Configuring SRX Series Service Gateways* on hand (freely available at www.juniper.net/dayone) for reference and in-depth discussions about the basic concepts of how to configure and monitor SRX devices.

After Reading This Booklet, You'll be Able To

- ✓ Perform the initial setup configuration of your SRX device.
- ✓ Configure basic system properties like users, DNS, SNMP, DHCP and Routing.
- ✓ Use J-Web to configure device security features like Zones, Screens, Policies, and NAT.
- ✓ Use J-Web to monitor network performance, upgrade software, and diagnose network problems.

NOTE The SRX Series Services Gateway is an eye-ful to read. This book simplifies the terminology by using the generic term *SRX*, or *the SRX*.

IMPORTANT The J-Web options shown in this chapter, and this book, differ depending on the device model, the OS version, and your installed licenses. Use this book's screen captures as guidelines for what might appear on your device's J-Web interface.

Wizards in 10.4 and above

Starting in Junos v10.4, the SRX includes a set of wizards to help you get the device configured, secure, and running right out of the box. When you first connect your lap top to the SRX, and log in to J-Web, you'll be presented with the Initial Startup wizard.

Chapter 1 begins with the Initial Setup wizard and walks you through that first configuration.

Subsequent chapters will show you how to access the other wizards by way of the J-Web interface and use them to configure firewall policies, NAT, and IPSec VPNs. You can also use J-Web to monitor and then adjust the settings of your SRX.

Following Along on Your SRX

This book was designed for you to follow along with it using J-Web. Use a SRX device or a sample test-bed to practice while reading. You'll be able to follow this book's instructions more easily if you have it open in print, or as an eBook, or as a PDF file on another screen or device beside your operational J-Web client.

MORE? *Day One: Deploying SRX Series Services Gateways*, by Barney Sanchez (available freely at www.juniper.net/dayone) is a companion book to this one. It goes into significant detail about configuring your SRX device, and covers all SRX devices from branch to enterprise service gateways.

EXPLORE Look for this page element to give you suggestions about topics to explore on your own time and on your own SRX device.

Chapter 1

Start Up, Connect, Log In

<i>Starting Up Your SRX</i>	<i>7</i>
<i>Starting J-Web</i>	<i>7</i>
<i>The Initial Setup Wizard</i>	<i>9</i>
<i>Taking a Tour of J-Web.....</i>	<i>18</i>
<i>Exploring the J-Web Tabs.....</i>	<i>20</i>

The J-Web interface allows you to configure, monitor, troubleshoot, and manage your device by means of an HTTP or HTTPS-enabled web browser. The built-in wizards make the initial setup, as well as configuring firewall policies, NAT, and IPSec VPNs, easy and intuitive to complete. Figure 1.1 shows a typical Dashboard view from J-Web.

Screen captures may differ on your device depending on your model and installed licenses.

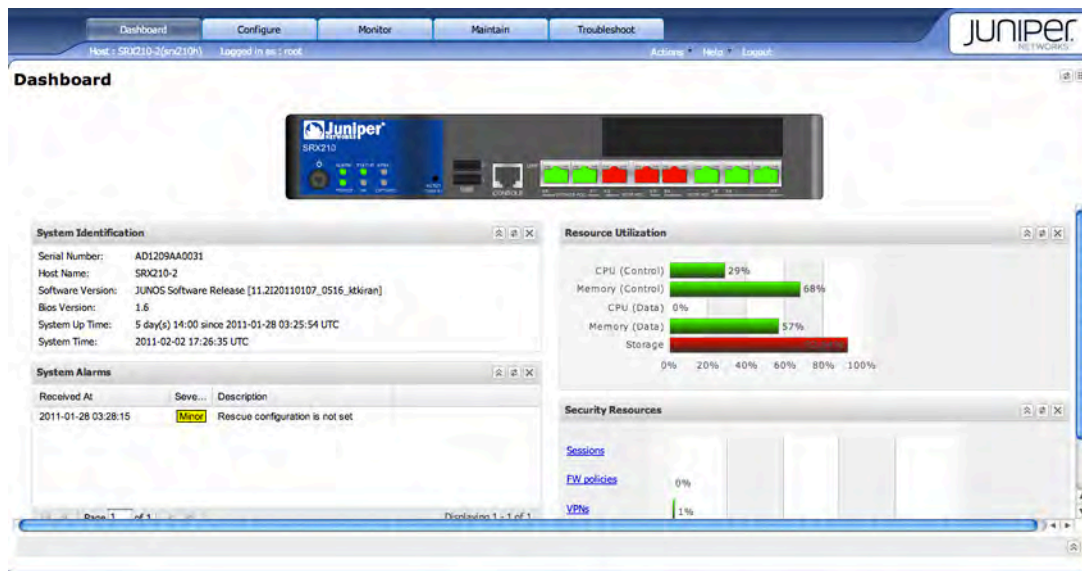


Figure 1.1 A Typical Dashboard View of J-Web

J-Web provides access to all the configuration statements supported by the device, so you can fully configure the device. You can perform all the following tasks with J-Web:

- **Scan System Status:** The J-Web Dashboard displays a graphical image of the chassis and interfaces, provides an easy way to identify the system, and an ad hoc view of resource utilization, security resources, system alarms, file usage, login sessions, chassis status, threat activity, and storage usage.
- **Monitor System Activity:** Displays the active configuration, as well as information about system events, alarms, interface status, security features, routing protocols, DHCP services, and much more.

- **Configure Routing and Security:** J-Web helps you configure device routing, security, switching, services, and class of service (CoS) in an easy-to-understand tabbed GUI. J-Web also provides a configuration editor that enables you to view and edit the entire configuration in one file.
- **Maintain the Device:** J-Web provides simple tools to help you maintain logs, temporary and core (crash) files, and to schedule system reboots. You can easily manage and upgrade software packages and licenses. J-Web also allows you to save and use configuration history and to set a rescue configuration.
- **Troubleshoot Traffic:** Troubleshoot routing problems by running the ping or traceroute diagnostic tools. You can also set RPM probes, check on MPLS LSPs, L2 and L3 VPNs, and L2 circuits. The packet capture tool lets you collect and analyze control traffic by providing Hex and ASCII packet data right within J-Web or saved in a PCAP file for use with a 3rd-party analysis tool. J-Web also gives you a Java applet CLI terminal that lets you run UNIX commands and operational commands.

MORE? If you would like to learn more about how to configure your SRX device using the CLI, as well as in-depth set-up instructions, see this book's companion guide, *Day One: Configuring SRX Series Service Gateways* by Barney Sanchez. You can use that book's detailed guidance on configuring the SRX with the CLI. Get it free in PDF format at www.juniper.net/dayone/ along with instructions on how to download eBook versions, too.

Starting Up Your SRX

Use the *Quick Start Guide* that came with your SRX model to connect the device to your network and power it up for the first time. If you don't have it, or can't find it, go www.juniper.net/techpubs (then follow the links for your specific SRX model). Download the PDF and use it to physically connect your SRX to your network.

Starting J-Web

To start J-Web, you'll need to cable to the device:

1. Attach one end of an Ethernet cable to the Ethernet port on your computer, and the other end to the 0/1 (fe-0/0/1) port on the SRX.

2. Enable your computer's LAN adapter if it is currently disabled. On Windows, select Start > Settings > Network Connections > Local Area Connection. If the 'Enable' button is visible, click it to enable your local network adapter. A green ready light should appear above the port.

3. Open a browser, and enter the following IP address into the browser address bar:

`http://192.168.1.1`

4. Within a few seconds you should see the J-Web Log In screen shown in Figure 1.2.

5. Type in *root* in the Username field. Do not enter any value in the Password field. Click the Log In button. You will immediately be taken to the Initial Setup wizard as shown in Figure 1.3.



Figure 1.2 Logging In to J-Web

NOTE Branch SRX devices are pre-configured with the IP address range 192.168.0.0/24 for management access. This IP range is typically set aside for router management access. For example, if you have a wireless router at home, you can open a browser and enter 192.168.0.1 into your browser's address bar to display your home router's management service.



Figure 1.3 The Initial Setup Wizard Initial Page

The Initial Setup wizard gets you up and running. It lets you set up basic information like IP address, default gateway, interface groups, and other settings. Before you click on Start, note the following.

The process consists of filling in the correct information in the correct fields and you should be prepared to have that basic information in front of you to complete the wizard set-up.

You can chart your process through the Initial Setup wizard by observing the left-hand column. Also in the left column note the brief instructions for completing each page of the wizard. If you click on an item under the Resources heading, it opens a new tab in your browser. Note you might have to maneuver back and forth between tabs to read the resource while completing the wizard pages.

The Initial Setup Wizard

Click on the Start button shown above in Figure 1.3 to begin the initial setup configuration of your SRX device.

Step 1: Configure System Identification

1. Fill out the four fields shown in Figure 1.4:

Host Name

Domain Name

Root Password

Verify Root Password

Juniper Web Device Manager

Initial Setup

Host: NoName(srx210r-p-m) Logged in as: root Help Logout

Setup Wizard

- Introduction
- System
- Identification**
- Network
- Interfaces
- J-Web preferences
- Time Management
- Review & Commit

About this page

Complete this page to identify your device on the network and set a password for the root user. Click a field name to get information about the field.

[SRX 210 Quickstart and Hardware Guides](#)

Configure System: Identification

Identification

Hostname * mysrx

Domain name myoffice.com

Root password * *****

Verify root password * *****

Back Next

Figure 1.4 The System/Identification Page

2. Give your device a name, type in your domain name, and provide a password and verify it. Since this is a networking device that provides security services, best practice is to provide a secure password. Make sure you have a safe place to archive the name and password of the device.
3. Click the Next button when complete.

Step 2: Configure Network Settings

1. Fill out the fields shown in Figure 1.5, starting with the Default Gateway. If DHCP is configured, leave the gateway field blank and the device will use the gateway pushed by DHCP.
2. The wizard should fill in the DNS Name Servers from the default configuration. If you want to add additional DNS Servers, or change the ones the wizard configured, simply type in the DNS address in the DNS Name Servers field, and click the Add button. To delete DNS servers, highlight them and click the Delete button. Notice you can highlight a DNS server and then move its order up or down.
3. Perform the same process for the Domain Search fields adding , deleting, or changing their order.

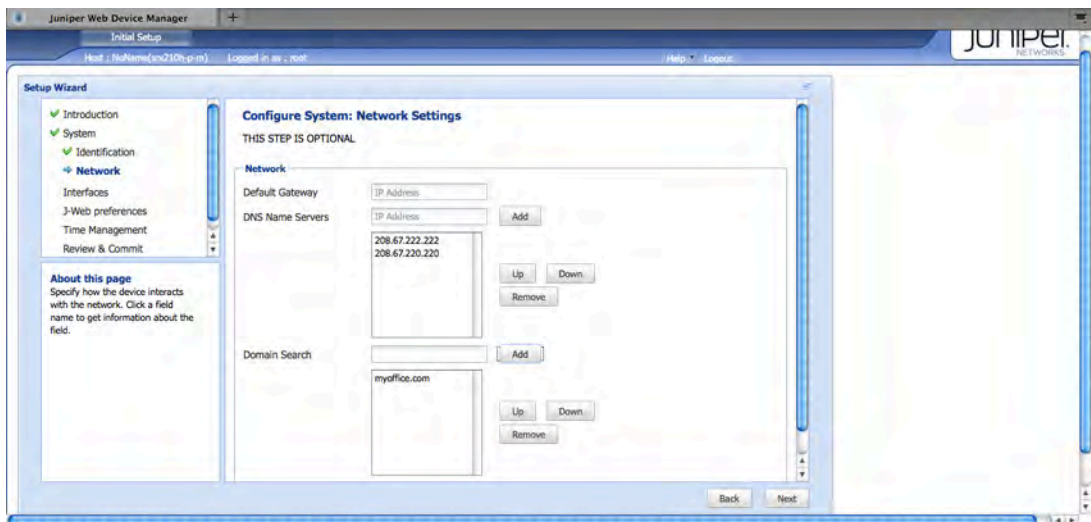


Figure 1.5 The Network Settings Page

TIP If you want information about a field name, click on the name itself.

4. Click the Next button when complete.

Step 3: Configure Interface Groups

The next page is optional and it helps you to configure interface groups. Depending on which SRX device model you are configuring, you may have more or less interfaces than the one shown in Figure 1.6. All interfaces except ge-0/0/0 (fe-00/0 for SRX100) are in a group called *vlan-trust* and have a single IP address.

This page is for creating multiple interface groups/vlans.

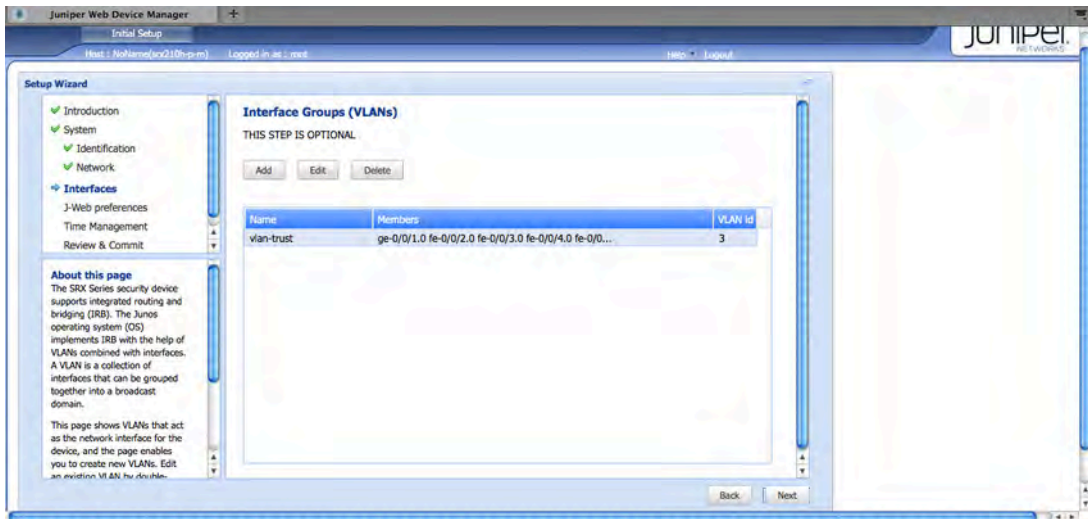


Figure 1.6 The Interface Groups (VLANs) Page

1. To create a new group you must first delete some of the interfaces from the *vlan-trust* group. Click **Edit**. Highlight the interfaces you want to move in the **Interfaces in Group** field and click the left arrow to move them into the **Available Interfaces** field. (These steps are not shown, by the way.) Click **Save** in the lower right and you'll return to the page shown above.
2. Now click on **Add**. Give the group a name. Highlight the interfaces in the **Available Interfaces** field and move them into the **Interfaces in Group** field by using the arrows. Click **Save** and you'll see the new group added to the page, as shown in Step 4's Figure 1.7.
3. Click the **Next** button when complete.

Step 4: Configure Interfaces

This page shows you the interfaces that you can assign an IP address to, and it is optional. Again, depending on which SRX device model you are configuring, and how you are setting it up, you may have more or less interfaces than the one shown in Figure 1.6.

Figure 1.6 shows two interfaces, the group `vlan-trust`, and the `ge-0/0/0.0` interface, which is the Internet-facing interface, and thus, an untrust security zone.

1. Highlight the interface you want to edit and click the Edit button (proceed to Step 5).

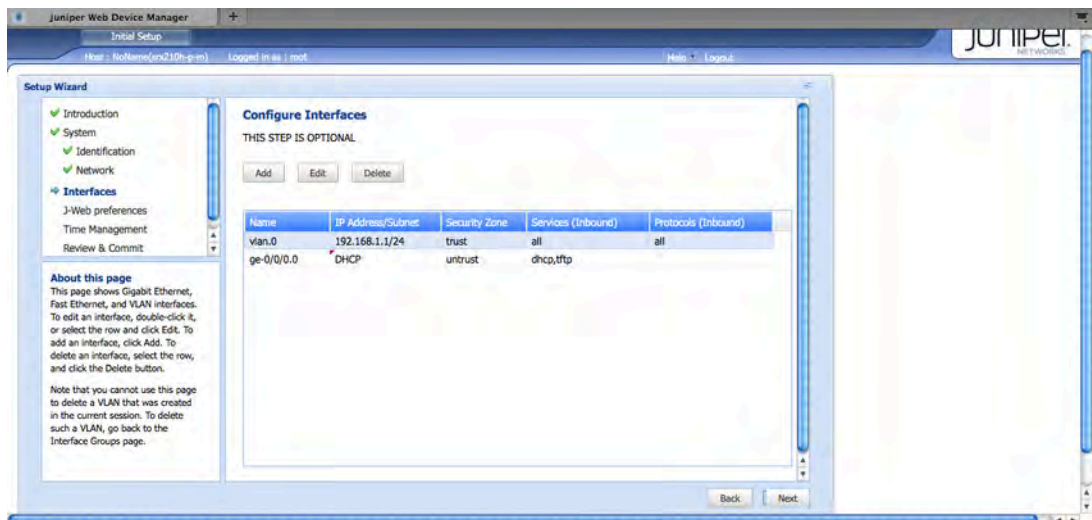


Figure 1.7 The Configure Interfaces Page

TIP If you need to delete a VLAN, you must click the Back button, delete it using the process in Step 3, Save, and then step forward again to this page in the wizard.

Step 5: Edit Interfaces

1. Fill out the fields shown in Figure 1.8 to configure the interface with the properties you want.
2. Note that you must click on either the DHCP or IP Address radial buttons for address fields to appear on the page.
3. Assign a security zone to the interface: trust, untrust, etc.
4. Choose the services and protocols you want assigned to this interface.

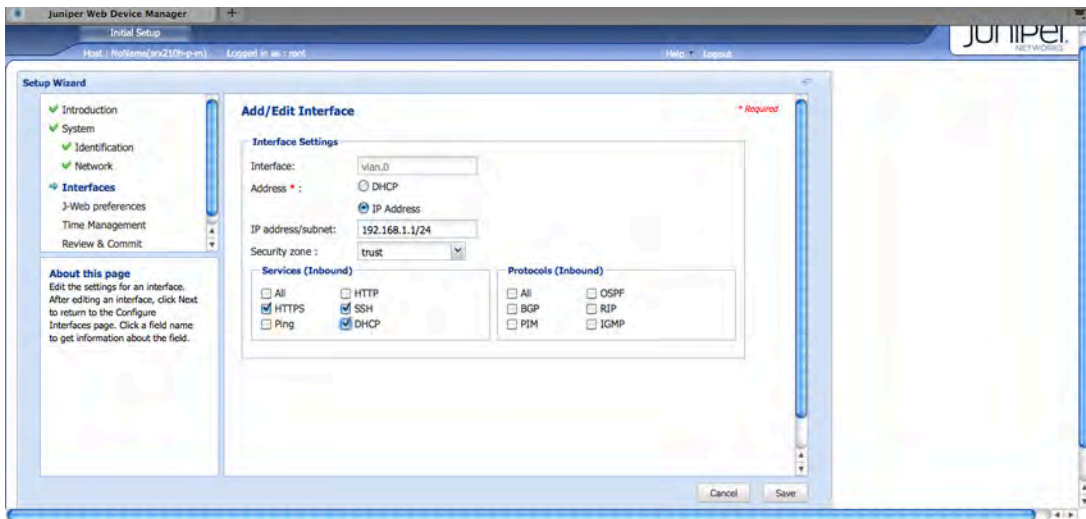


Figure 1.8 Add/Edit Interfaces Page

5. Click Save in the lower right.
6. You will return to the Configure Interfaces page shown in Step 4's Figure 1.6.
7. Click Next.

Step 6: Configure J-Web Preferences

Use this wizard page to set some basic preferences for J-Web. The device defaults should work well for you.

1. Choose how you want to start J-Web each time to launch it.
2. Choose your commit options. Again, the default shown in Figure 1.9 is a safe method of committing.

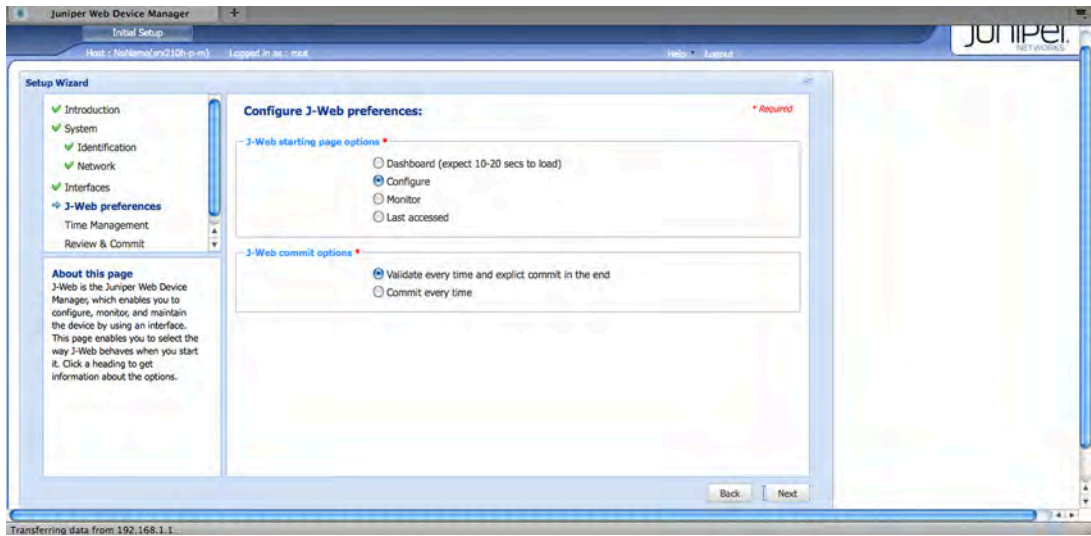


Figure 1.9 Configure J-Web Preferences Page

3. Click the Next button when complete.

Step 7: Configure System Time

Will this wizard page you can manually set the system time or change or add NTP servers.

1. If the current system time is incorrect, you can reset it manually, as shown in Figure 1.10.
2. Set the Time Zone.
3. If necessary you can add NTP servers.

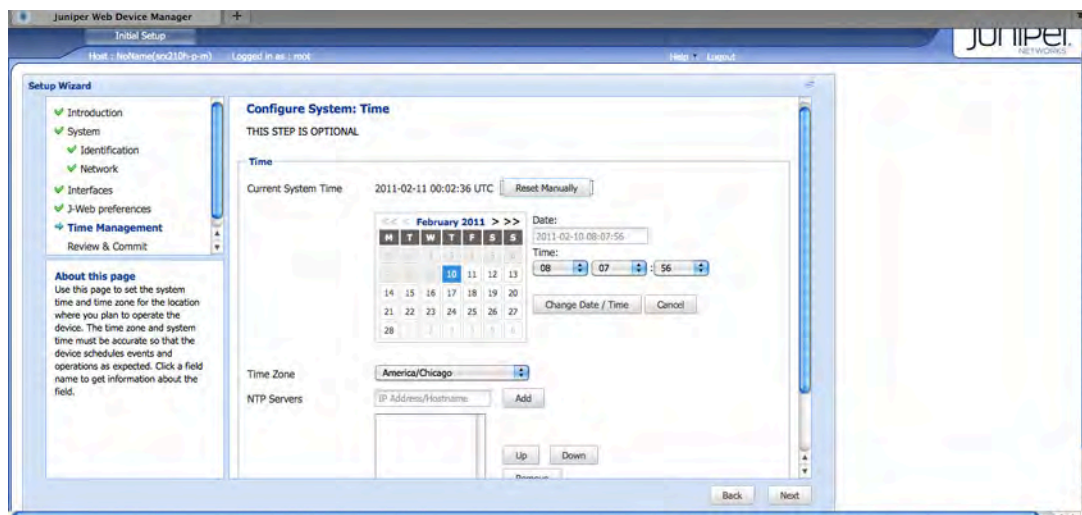


Figure 1.10 Configure System Time Page

4. Click the Next button when complete.

Step 8: Review and Commit

It's time to pause and review your Initial Setup configuration, as shown in Figure 1.11, and commit.

Note that the rest of this book will show you how to use J-Web to tweak, configure, and monitor your SRX device, so this is not the last chance to configure things.

TIP Are you sure you have the correct password archived somewhere?

1. Review the system settings. If you need to, click on the blue headers to make changes to that group of settings.

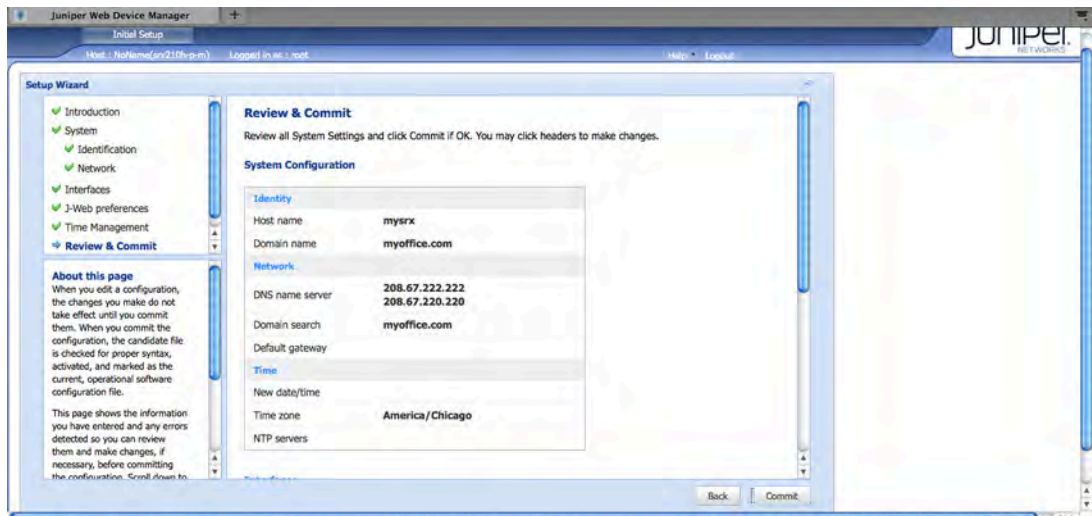


Figure 1.11 Configuration Review and Commit

2. If you are satisfied, click on the Commit button.

That's it! You have successfully performed the initial setup of your SRX!

Taking a Tour of J-Web

Now that you've performed the initial configuration of your SRX using the Initial Startup wizard, let's take a tour.

Whenever you log on via a browser to J-Web, you'll see a simple monitoring interface that provides information at-a-glance to the administrator. J-Web also displays a graphical image of the specific SRX device it is connected to, as shown in Figure 1.12. Once again, note that the image on your J-Web interface may vary due to differences in SRX models and configuration.

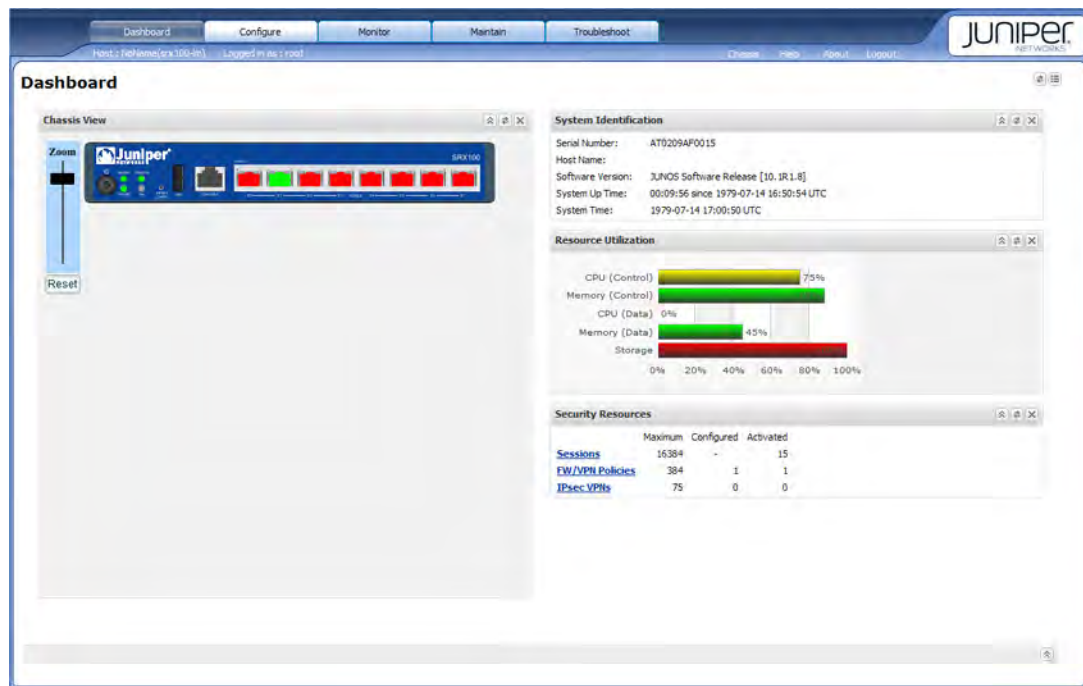


Figure 1.12 Reviewing the J-Web Dashboard Statistics

Note you can immediately see the device's system identification detail, its resource utilization in a color-coded chart (red meaning reaching limits), and security resources. You can rearrange the display modules to view the statistics that are most important to you, as you can see in Figure 1.13, in which the Chassis Status has been moved to the prominent upper quadrant of the page.

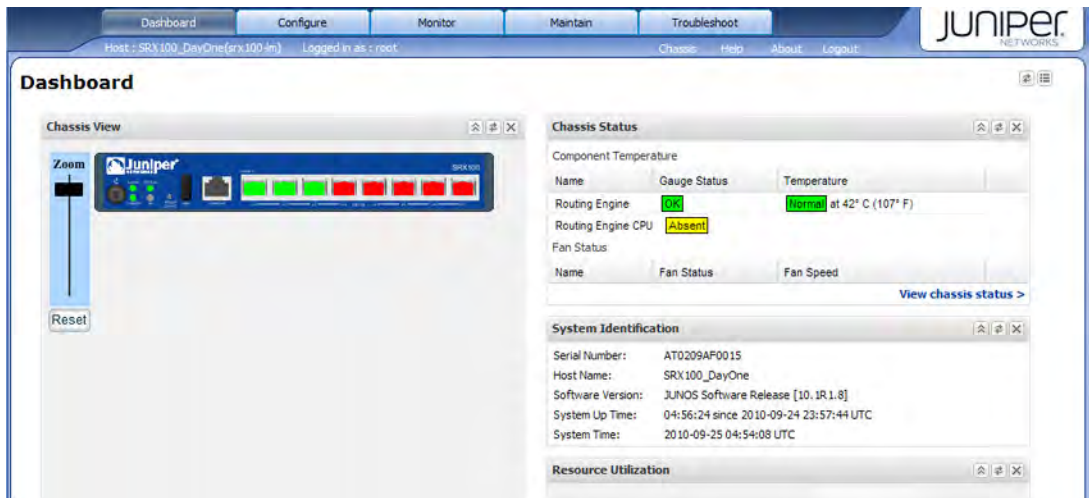


Figure 1.13 Reconfiguring the Dashboard Statistics Display

An interesting feature of the Dashboard is that you can hover your mouse pointer over the various interfaces of the SRX to see how they are configured. In Figure 1.14, you can see how the ge-0/0/0 interface is presented when hovering over the interface image with the pointer. You don't have to enter the CLI command `show interfaces` in J-Web. A quick swipe of your pointer can reveal all the various interface information. Note that some interfaces are green (active) and some are red (unused).



Figure 1.14 Displaying Individual Interface Configuration Commands

TIP Use the zoom sliders if you're using a small screened device to work in J-Web.

Exploring the J-Web Tabs

You'll probably want to take a quick tour of the Navigation tabs at the top of the J-Web Dashboard.

The Configure Tab

Click on the Configure tab to display the main configuration pages. As shown in Figure 1.15, the first thing you'll see is a list of interfaces and their current status, including their Link Status, IP Address, and Zone if applicable. Filtering tools at the top of the screen can help sort and display configuration details.

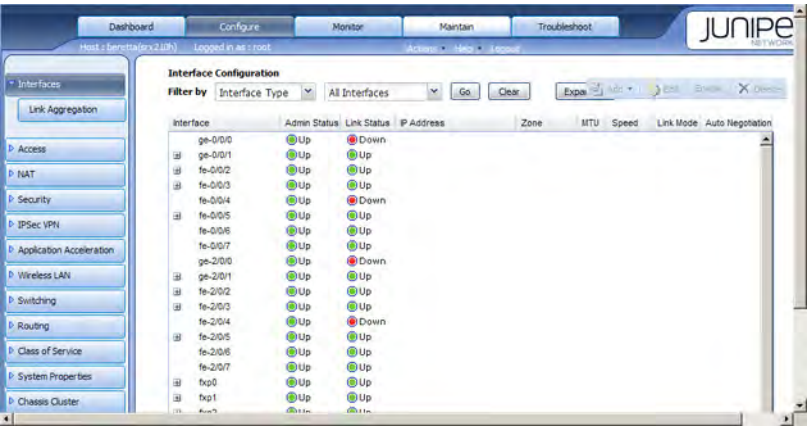


Figure 1.15 Viewing the Configure Tab and Interfaces Details

Along the left-side navigation panel, you'll see buttons that display configuration pages for a variety of security, routing, switching, and services options. All of the major SRX configuration options are here, conveniently located in one navigation menu.

Along the upper right corner of the page, a number of commands dynamically appear depending on the context of the current page, some of which are shown in Figure 1.16. The most common commands in this dynamic menu are:

- **Commit:** Attempts to commit the current configuration changes.
- **Chassis:** Click on this to view the Chassis image in a separate window.
- **Help:** Displays the online J-Web help pages. You must be connected to the Internet to access these pages.
- **Logout:** Ends your J-Web session.

The Monitor Tab

On the Monitor tab, you can track a variety of Junos and SRX statistics, alarms, and events, including traffic patterns, over individual interfaces.

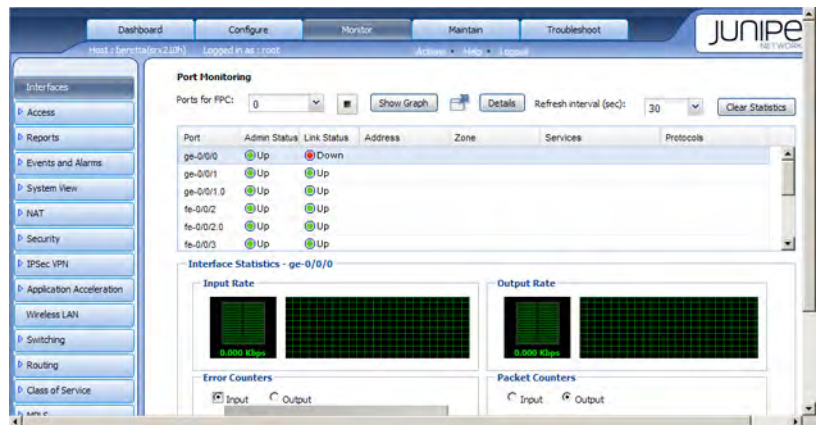


Figure 1.16 Monitoring Junos and SRX Statistics

The Maintain Tab

The Maintain tab is where you will find all of the utilities to keep your SRX device and software up-to-date, and where you can locate a variety of log files that your SRX device generates shown in Figure 1.17.

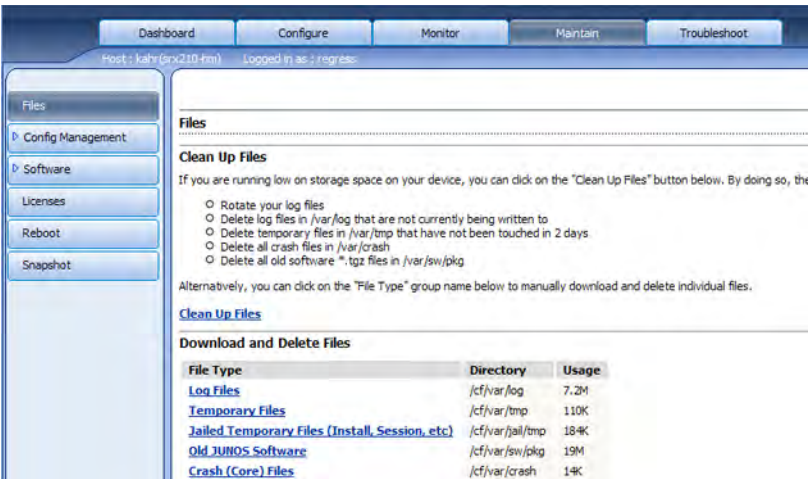


Figure 1.17 Maintaining the SRX Device

The Troubleshoot Tab

The Troubleshoot tab, shown in Figure 1.18, provides several powerful tools, like Ping, Traceroute, and a Java CLI editor, that help you analyze and resolve connectivity and traffic problems on your device.

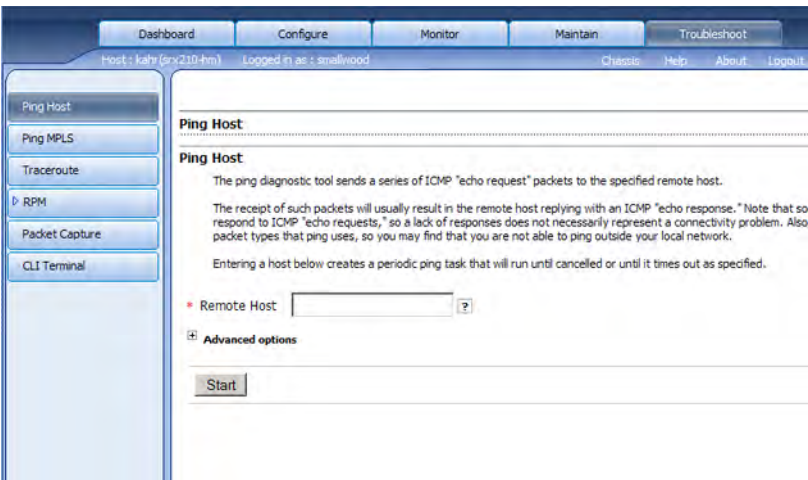


Figure 1.18 Troubleshooting the SRX Device

We're done. You've done the initial configuration and taken a tour. The rest of this book details the other wizards and some great J-Web tips.

Chapter 2

Configuring the SRX with J-Web Wizards

Configuring Firewall Policies with the J-Web Firewall Wizard . . 25

Configuring NAT with the J-Web NAT Wizard 27

Configuring an IPSec VPN with the J-Web VPN Wizard 28

In J-Web, you'll see several wizards in the Configure section. These wizards can help you configure the first few services, which will be important to complete before moving on to more complex services. These initial services are:

- Firewall Configuration
- IPSec VPN Configuration
- NAT Configuration

As you can guess, configuring these three services will protect your network from outside intruders and will help you provide secure access to your network resources only to the appropriate people.

You can find the wizards toward the bottom of the configuration tab buttons in the left-hand navigation menu, as shown in Figure 2.1.

On each wizard, you click the Launch button to begin.

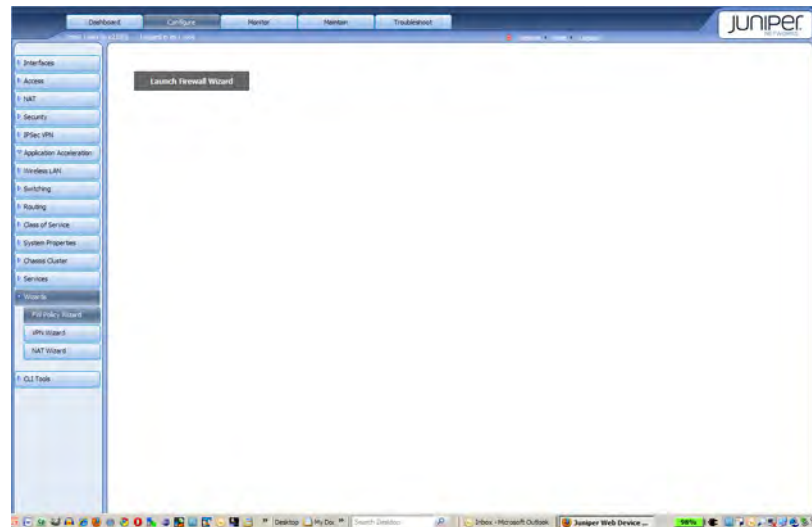


Figure 2.1 Starting Wizards with the Launch Button

Each Wizard contains a Help panel in the lower-left corner that provides valuable information about the current wizard page. You can click many items on the Wizard pages, including headings and element names, and the Wizard displays context-sensitive Help in the Help panel. The hierarchical view of steps in the upper-right panel is a form of breadcrumb that lets you know where you are in the process.

Configuring Firewall Policies with the J-Web Firewall Wizard

The Firewall Wizard helps you configure firewall policies. The SRX device provides zones and policies to help categorize and control different types of traffic as it attempts to reach your network. By default, when you first configure the SRX device, all traffic is denied. This is done to protect your network from attackers or malicious software before you have configured any real security on the device.

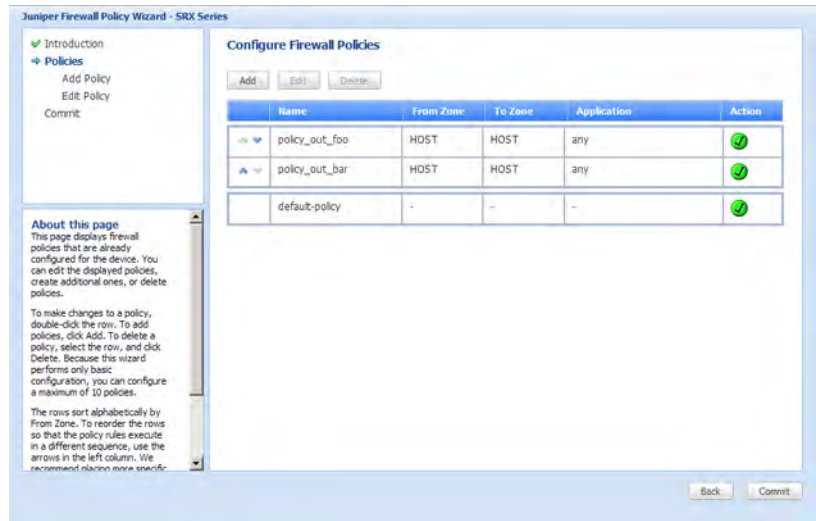


Figure 2.2 Configuring Firewall Policies

Policies help you control traffic to resources inside the firewall, based on a number of configurable criteria, including IP address, user, and interface. To begin configuring a new firewall policy, click the Add button (as shown in Figure 2.2) and you'll see something similar to Figure 2.3.

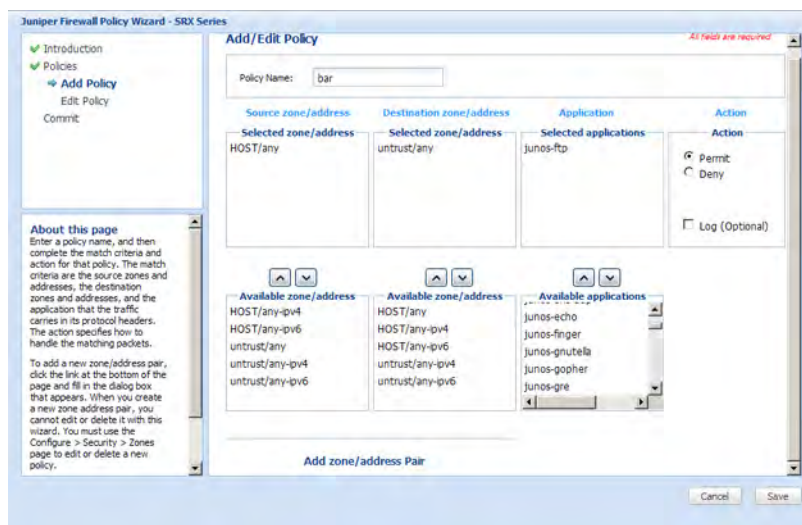


Figure 2.3 Configuring the Policy Name, Zones, Applications, and Actions

In the first three boxes, from left to right, you can add a source zone, a destination zone, an application, and a corresponding action. In the example shown in Figure 2.3, the Source zone is defined as HOST/any, and the Destination zone is defined as untrust/any. The Application, in this case, is FTP, and the Action is set to Permit, meaning that somebody operating from the HOST zone is allowed to FTP to the untrust zone.

You can also add a zone/address pair, as shown in Figure 2.4, which allows you to associate a specific IP address with a zone. Configuring zone/address pairs can be very useful when enforcing the usage patterns for certain applications or access to specific resources by known address ranges. For example, if you have suppliers who have access to certain areas of your internal network, you could use the zone/address pair configuration to restrict any traffic from your suppliers' IP ranges.

Conversely, you could grant access to some specific IP address on a temporary basis, for example, to accommodate consultants or contractors.

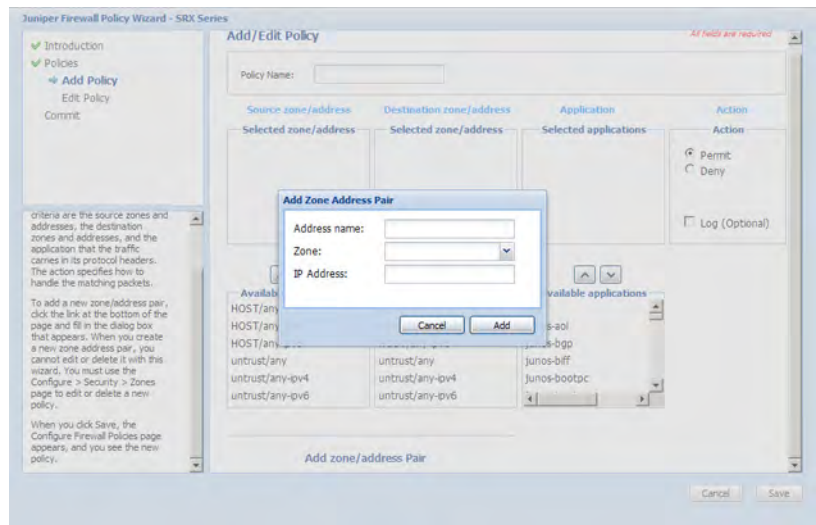


Figure 2.4 Adding a Zone Address Pair

Configuring NAT with the J-Web NAT Wizard

The NAT Wizard helps you configure Network Address Translation (NAT), which is the service that translates addresses so they can be understood inside and outside your network. Since internal networks typically use a different class of IP address than external addresses, NAT performs the necessary functions to help direct traffic to the correct location, and to shield internal addresses from external traffic, among other things. You can configure source, destination and static NAT using the wizard. The NAT wizard includes some simple network diagrams, as shown in Figure 2.5, to help you visualize your network when configuring NAT.

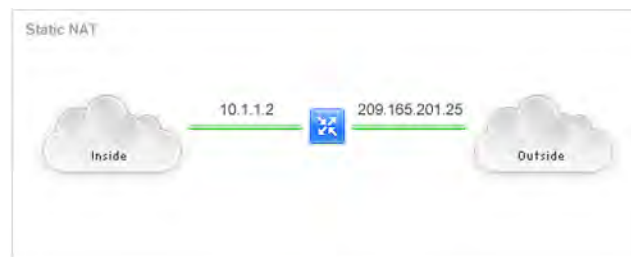


Figure 2.5 Visualizing Network Configuration for NAT

After launching the NAT wizard, you'll be able to add NAT rules for source, destination, and static NAT. For example, Figure 2.6 shows the Destination NAT Add Rule page. Note the online help in the lower left corner of the page. Clicking on headings, like Rule Name will display more information about what the wizard needs you to add.

Figure 2.6 Configuring Destination NAT Rule

Configuring an IPSec VPN with the J-Web VPN Wizard

The VPN wizard provides you a way to configure IPSec VPNs that allow your employees to remotely access your network in a completely secure manner. You can also configure site-to-site VPNs, which are route-based rather than policy-based. The J-Web VPN wizard walks you through the steps necessary to configure these types of IPSec VPNs.

After launching the VPN wizard, you'll be presented with a page showing a sample network diagram, to help you visualize your remote access requirements. On this screen, you'll be able to select the different types of VPN, as you can see in Figure 2.7.

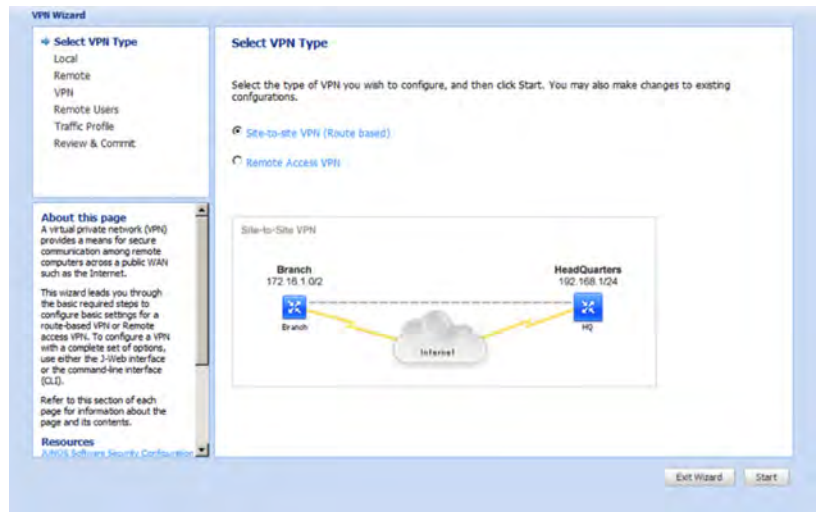


Figure 2.7 Selecting the VPN Type on the J-Web VPN Wizard

To configure a remote access VPN, select the Remote Access VPN option as shown in Figure 2.8.

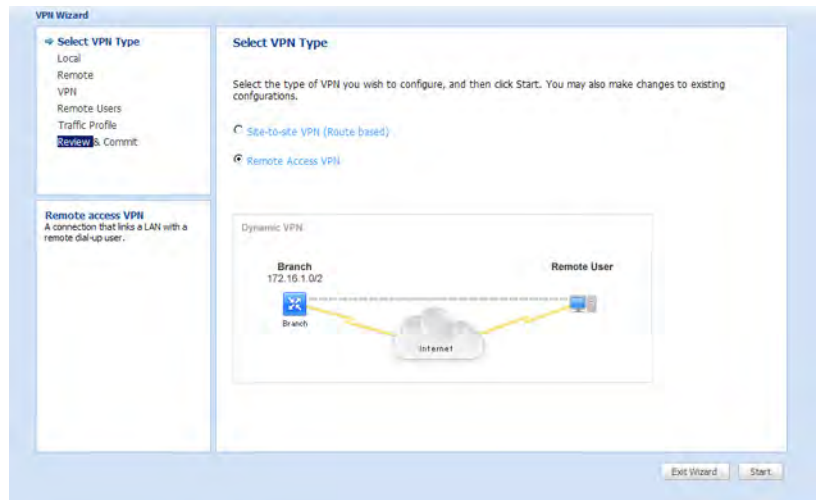


Figure 2.8 Configuring the Remote Access VPN

You'll need to provide a VPN name, a zone, the network addresses, which interface you want VPN traffic to traverse, and the interface zone, as illustrated in Figure 2.9.

The screenshot shows the 'VPN Wizard' interface in J-Web. On the left, a sidebar contains a progress indicator with four steps: 'Select VPN Type' (checked), 'Local' (selected), 'VPN Users', 'Remote Users', and 'Review & Commit'. Below this is an 'About this page' section with explanatory text and a small diagram of a VPN tunnel. The main area is titled 'Remote Access VPN: Local Settings' and includes a red note stating '* All fields are required'. The configuration fields are as follows:

- Name:** A text field containing 'foo'.
- Protected Networks:** A section with a 'Zone' dropdown set to 'HOST' and a 'Network(s)' list. The list contains '10.157.162.1/24'. There are 'Add' and 'Remove' buttons next to the list.
- Public Network:** A section with an 'Interface' dropdown set to 'ge-0/0/0.0' and an 'Interface Zone' dropdown set to 'HOST'.

At the bottom right of the main area are 'Back' and 'Next' buttons.

Figure 2.9 Configuring the Remote Access VPN Local Settings

Additionally, you'll need to provide VPN settings, as shown in Figure 2.10. The remote access VPN configuration requires that you choose an IKE security level, provide a predefined IKE key, remote identify, and the type of IKE ID, whether group or shared. You must also choose an IPSec security level, and an IPSec Perfect Forward Secrecy group.

VPN Wizard

- Select VPN Type
 - Local
 - VPN
 - Remote Users
 - Review & Commit

About this page
Identify the outgoing interface for a remote access VPN. On this page you specify the local private network and the public network through which the tunnel passes. Click a field name to get information about the field.

Remote Access VPN: Local Settings * All fields are required

Name
VPN Name *

Protected Networks

Zone *

Network(s) * Example: 1.2.3.0/24

Public Network

Interface *

Interface Zone *

Figure 2.10 Configuring VPN Settings

In Figure 2.11, you can see how to define remote users. On the Remote Users page of the VPN Wizard you define your users' authentication credentials. You must also supply an IP pool address, which will serve as the address pool for other VPNs defined on this device.

VPN Wizard

- Select VPN Type
 - Local
 - VPN
 - Remote Users
 - Review & Commit

About this page
Describe the settings for the remote user of the remote access VPN. Click a field name to get information about the field.

Remote Access VPN: Remote User Settings * Required

Authentication

Same credentials used for Xauth and authentication for client download. At least one user must be created.

User Name	Password
smallwood	*****

IP Settings

IP Pool (for Config Mode) * Note: The pool settings are shared by multiple VPN's

DNS Server

WINS Server

Figure 2.11 Configuring Your Remote Users' Authentication Credentials

All of the wizards provide a review page where you can check to make sure that you've configured everything correctly. After completing each wizard, you should commit the configuration by clicking the Commit button, as shown in Figure 2.12.

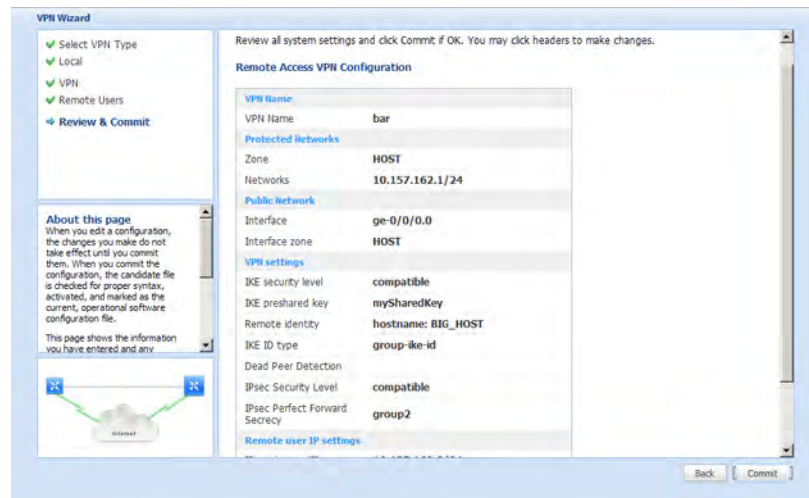


Figure 2.12 Reviewing and Committing the Wizard Configurations

Once you go through a few of the wizards, they will be self-evident and easy to configure, review, and commit. The rest of this book will show you how to use J-Web's interfaces in a non-wizard way, so you tweak, monitor, and troubleshoot your SRX device.

IMPORTANT Remember that the J-Web options shown in this chapter, and this book, differ depending on the device model, the OS version, and your installed licenses. Use this book's screen captures as guides for what might appear on your device's J-Web interface.

Chapter 3

Configuring the SRX Device

<i>Configuring Management Access</i>	<i>34</i>
<i>Configuring System Properties and DNS</i>	<i>35</i>
<i>Configuring Administrator Accounts.....</i>	<i>36</i>
<i>Configuring Date and Time.....</i>	<i>39</i>
<i>Configuring the SNMP Agent.....</i>	<i>40</i>
<i>Configuring DHCP Settings</i>	<i>42</i>
<i>Configuring Basic Alarms</i>	<i>44</i>
<i>Upgrading Software and Rebooting.....</i>	<i>45</i>
<i>Uploading Licenses</i>	<i>46</i>

This chapter shows you how to configure the basic SRX device properties including system identification, DNS, DHCP, date and time, management access, administrator accounts, SNMP, software upgrades, and uploading license files. Log in to your device or get your test bed fired up and let's get started.

MORE? If you need more information during any of these tutorial steps refer to your SRX device's documentation, freely available at www.juniper.net/techpubs.

Configuring Management Access

First, you need to configure secure management access to your device. To communicate with the device, the J-Web interface (by default) uses Hypertext Transfer Protocol (HTTP). HTTP allows easy web access but no encryption, so any data transmitted between your web browser and the device over HTTP is vulnerable to interception or attack.

To ensure secure web access, the SRX Series devices support Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

Before you begin the configuration, note that you need to complete the following tasks:

- Establish basic connectivity.
- Obtain an SSL certificate from a trusted signing authority.

IMPORTANT Remember that the J-Web options shown in this chapter, and this book, differ depending on the device model, the OS version, and your installed licenses. Use this book's screen captures as guides for what might appear on your device's J-Web interface.

To Configure the Management Access Properties

1. Select Configure tab > System Properties > Management Access as shown in Figure 3.1.
2. Click the Edit link in the far right of the screen.
3. Select the Services tab, enable HTTP, and select the interface.

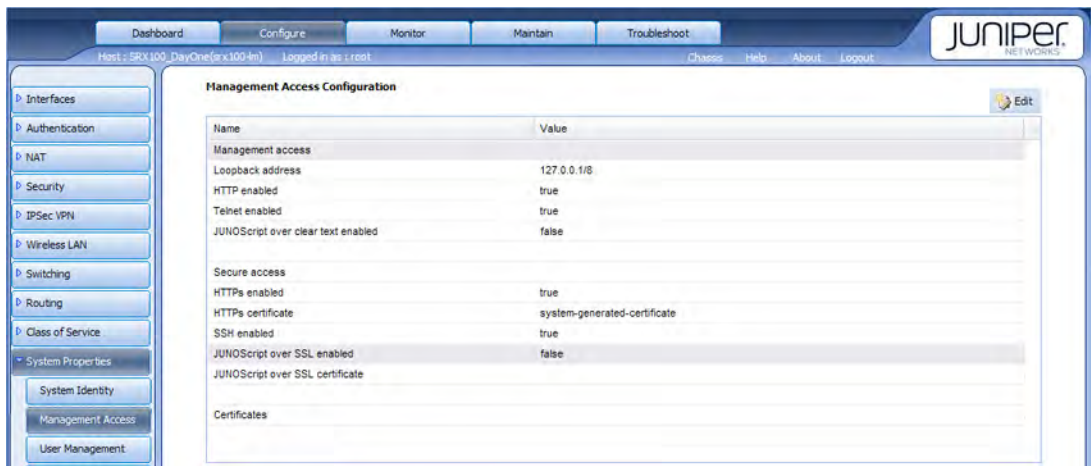


Figure 3.1 Configuring Management Access

- NOTE** If you selected HTTPS, first go to Certificates tab and add the certificate, then select Services tab, select the certificate, and the interface.
4. Click OK.
 5. Click Commit.

Configuring System Properties and DNS

Next, let's configure the essential system properties such as hostname, domain name, root password, DNS servers, and domain search.

To Configure the System Properties

1. Select Configure tab > System Properties > System Identity as shown in Figure 3.2.

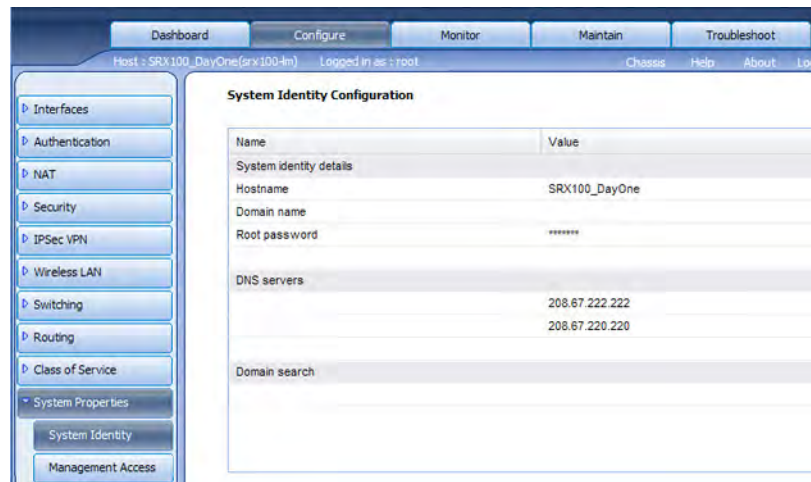


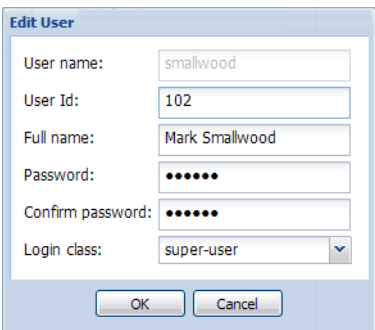
Figure 3.2 Configuring System Properties

2. Click the Edit link at the far right of the screen.
3. Enter the hostname, a root password, and then confirm the password in the J-Web fields.
4. Add one or more DNS servers.
5. Enter a domain name for the SRX device.
6. Add one or more domain prefixes to search in order to resolve local hosts.
7. Click OK.
8. Click Commit.

Configuring Administrator Accounts

J-Web allows managing system functions, including RADIUS and TACACS+ servers, as well as configuring user login accounts. First let's provide a little background before adding users.

As shown in Figure 3.3, user accounts provide one way for users to access the SRX device (users can also access the device without accounts if configured in RADIUS and TACACS+). Here, the device creates a home directory after the user is created. By default, an account for the *root* user is always configured.



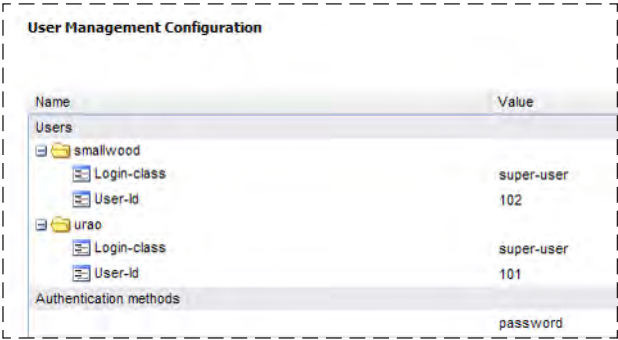
The 'Edit User' dialog box contains the following fields and values:

Field	Value
User name:	smallwood
User Id:	102
Full name:	Mark Smallwood
Password:	•••••
Confirm password:	•••••
Login class:	super-user

Buttons: OK, Cancel

Figure 3.3 Creating New Users with Local Authentication

All the users who log in to the SRX device must be in a Login class. You can use the predefined Login classes: *operator*, *read-only*, *super-user*, and *unauthorized*, or create a new Login class. You then apply one Login class to an individual user account. Figure 3.4 shows that you can manage user accounts at any time, and add and change Login classes.



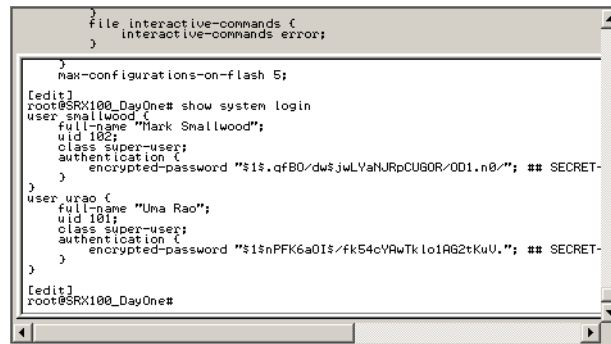
User Management Configuration	
Name	Value
Users	
smallwood	
Login-class	super-user
User-Id	102
urao	
Login-class	super-user
User-Id	101
Authentication methods	password

Figure 3.4 Reviewing User Accounts in J-Web

- Junos supports three methods of user authentication:
- Local password authentication
 - Remote Authentication Dial-In User Service (RADIUS)
 - Terminal Access Controller Access Control System Plus (TACACS+)

With local password authentication, you configure a password for each user allowed to log in to the SRX device. RADIUS and TACACS+ are authentication methods for validating users who attempt to access the device using Telnet. Both are distributed client/server systems – clients run on the device, and the server runs on a remote network system.

You can configure the device to use RADIUS or TACACS+ authentication, or both, to validate users who attempt to access the device. If you set up both authentication methods, you can also configure which method the device tries first.



```

}
file interactive-commands {
}
interactive-commands error;

}
max-configurations-on-flash 5;

[edit]
root@SRX100_DayOne# show system login
user_smallwood {
  full-name "Mark Smallwood";
  uid 102;
  class super-user;
  authentication {
    encrypted-password "$1$.qfB0/dw$jwLVahJRpCU60R/OD1.n0/"; ## SECRET-
  }
}
user_urao {
  full-name "Uma Rao";
  uid 101;
  class super-user;
  authentication {
    encrypted-password "$1$nPFK6a0I$/fk54cYAwTk lo1A62tKuU,."; ## SECRET-
  }
}

[edit]
root@SRX100_DayOne#

```

Figure 3.5 Reviewing Login Accounts in the CLI

To Add New Users to Your SRX Device

1. Select the Configure tab > System Properties > User Management.
2. Click the Edit button on the upper-right side of the page.
3. Select the Users tab, then click the Add button.
4. Enter the User name, password, confirm the password, and the Login class.
5. Click OK.
6. Select the Authentication Method and Order tab to configure different types of authentication and the order in which the device processes users.
7. When you're done, click OK.
8. Click Commit.

Configuring Date and Time

Every Juniper device contains an internal clock that continually operates while the device is powered on. You can manually set the clock from J-Web, and ideally, you would configure your firewall to connect to a timeserver using Network Time Protocol (NTP) for accurate time stamping, as shown in Figure 3.6.

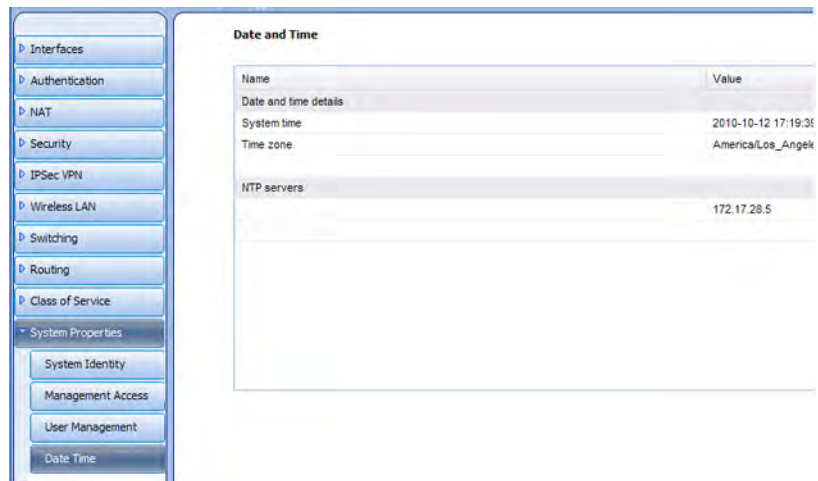


Figure 3.6 **Setting Date and Time**

BEST PRACTICE The time settings on your network devices need to be synchronized in order to avoid frame slips or *drift*. Best practice calls for you to use one time source only. So, whichever time server you select, it should be the same time server you select to set date and time on *all* of your devices.

To Set the SRX Clock to the Correct Time

1. Select the Configure tab > System Properties > Date Time.
2. Click the Edit link to see the Edit Date and Time Settings window as shown in Figure 3.7.
3. Select the correct time zone for your location.
4. Set time either to Synchronize with PC, NTP, or Manual. If you select NTP, add the NTP server IP Address.

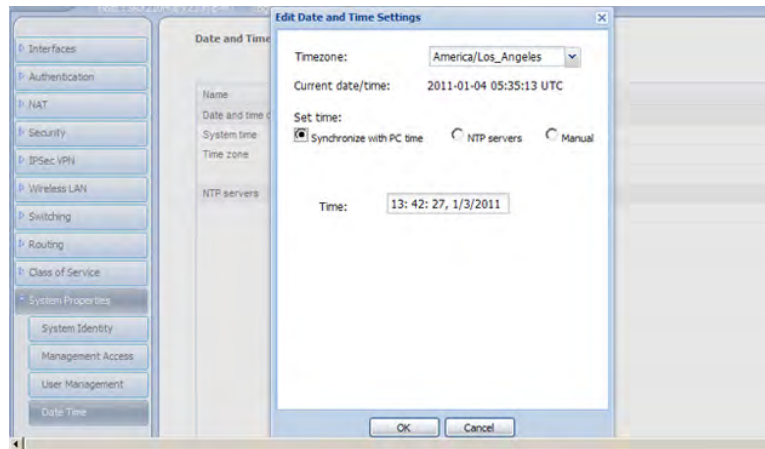


Figure 3.7 Adding NTP Servers and Server Pools

5. Click OK.
6. Click Commit.

Configuring the SNMP Agent

Simple Network Management Protocol (SNMP) allows remote administrators to view data statistics on a Juniper device. It also allows a Juniper device to send information to a central server. J-Web configuration allows you to define system identification information, create SNMP communities, create SNMP trap groups, and configure health monitor options. Figure 3.8 shows the J-Web configuration page for SNMP.

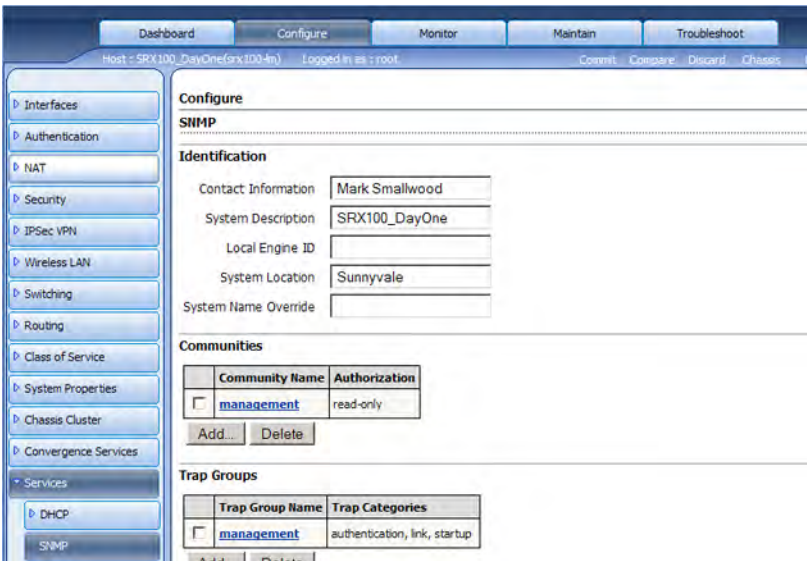


Figure 3.8 SNMP Configuration Page

To Configure SNMP on Your SRX Device

1. Select the Configure tab > Services > SNMP.
2. Enter the appropriate information for the Identification, Communities, Trap Group, and Health Monitoring fields. Figure 3.9 is a detail of the Traps Group Page.

The screenshot shows the 'Configure' window for an SNMP Trap Group. The window has a title bar 'Configure' and a sub-header 'SNMP'. Below this is the 'Traps' section. It contains a text field for 'Trap Group Name' with the value 'SRX_Trap_One'. To the right of this field is a list of categories with checkboxes: 'Authentication' (unchecked), 'Chassis' (checked), 'Configuration' (unchecked), 'Link' (checked), 'Remote operations' (unchecked), 'RMON alarm' (unchecked), 'Routing' (checked), 'Startup' (unchecked), and 'VRRP events' (unchecked). Below the categories is a 'Targets' section with a text area containing the IP addresses '192.168.1.2' and '192.168.1.3'. To the right of the text area is a help icon (?). Below the text area are 'Add' and 'Delete' buttons. At the bottom of the window are 'OK' and 'Cancel' buttons.

Figure 3.9 Configuring an SNMP Trap Group

3. Click OK.
4. Click Commit.
5. When you have configured trap groups, communities, and health monitoring, click the Apply button.
6. To confirm your configuration, click Commit.

Configuring DHCP Settings

A Dynamic Host Configuration Protocol (DHCP) server automatically allocates IP addresses and delivers configuration settings to client hosts on a subnet. DHCP lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network, so you can use a limited (smaller) number of addresses.

An IP address can also be leased to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses among a group of hosts that do not need permanent IP addresses.

Your SRX Series device can act as a DHCP server, providing IP addresses and settings to hosts, such as PCs that are connected to device interfaces.

NOTE The DHCP server is compatible with the DHCP servers of other vendors on the network. The device can also operate as a DHCP client and DHCP relay agent.

Before you begin configuring the SRX device as a DHCP server, you should complete the following tasks:

- Determine the IP address pools and the lease duration to use for each subnet.
- Obtain the MAC address of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- Determine the DHCP options required by the subnets and clients in your network.

Write these tasks down or have them completed prior to configuring with J-Web.

To Configure the DHCP Server

1. Select the Configure tab > Services > DHCP.
2. Select the Global Settings tab.
3. Enter the Server Identifier, Propagate Interface, Name Server IP address, Gateway Routers, and WINS Server IP address in their appropriate fields.
4. Enter the Maximum Lease time, Default lease time, and Boot file and Boot Server information.
5. Click Apply.
6. Select the DHCP Pool tab, Enter Address Pool Subnet, Address Range Low, and Address Range High as shown in Figure 3.10.

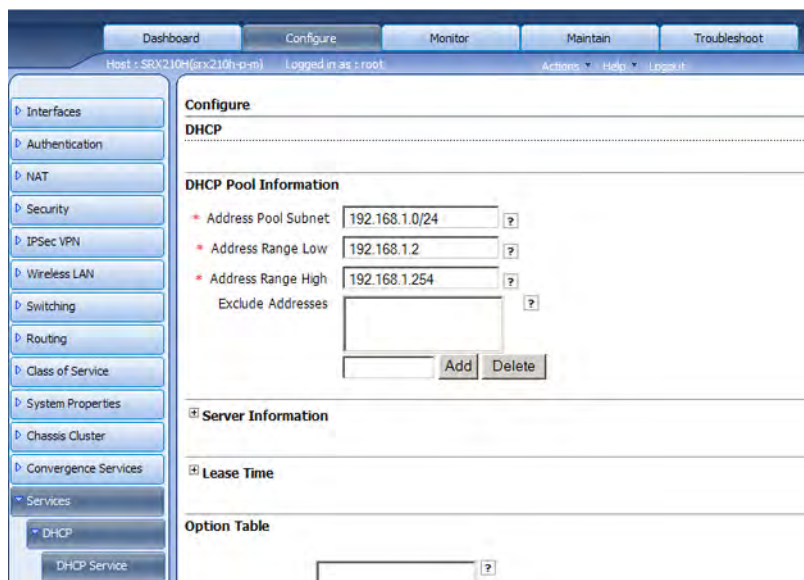


Figure 3.10 Configuring the DHCP Service

7. Click OK.
8. Select the Static Binding tab, enter the DHCP MAC Address, Host name, and add the Fixed Address.
9. Click OK.
10. Click Commit.

Configuring Basic Alarms

The SRX supports a number of system and chassis alarms that help to monitor the device environment and interface status, and J-Web provides a very simple way to configure alarms with the Point and Click CLI feature. Check it out.

To Configure a Basic Alarm

1. Select the Configure tab > CLI Tools > Point and Click CLI.
2. Click the Chassis Configure link.

3. Click the Alarm Configure link.
4. Click the Ds1 link (Ds1 is your T1 interface).
5. Select red from the Ylw drop-down menu.
6. Click OK.
7. Click the Ethernet link.
8. Select red from the Link Down drop-down menu.
9. Click OK three times.
10. Click Commit.

Now, when you monitor your device, you'll see a number of messages on the monitoring pages within the Monitor tab based on your chassis alarms, SNMP, interface alarms, and any other alarms you configure.

Upgrading Software and Rebooting

SRX Series Services Gateways are delivered with Junos preinstalled, so when you power-on the device, it starts (boots) using its primary boot device, typically an onboard Compact Flash card. The SRX also supports secondary boot devices, allowing you to back up your primary boot device and configuration.

The Junos release schedule is renown for its predictability, once a calendar quarter, year in and year out. Each new Junos release may include security updates, software fixes, or both, that are needed by your device. To continue to maintain the highest level of security, it's important that you remain updated and current with the most recent Junos release on your SRX device.

NOTE Before you begin to install a software upgrade, you'll need to obtain a valid Juniper Networks support contract. To obtain a web account, complete the registration form at the Juniper Networks website: <https://www.juniper.net/registration/Register.jsp>

ALERT! Before installing an upgrade, *back up* your primary boot device onto a secondary storage device. Best practice calls for you to verify that the available space on the Compact Flash card is large enough to accommodate the upgrade.

During a successful upgrade, the upgrade package completely reinstalls the existing software. It retains configuration files, log files, and similar information from the previous version.

To Install the Package from a Remote Server Using J-Web

1. Select the Maintain tab > Software > Install Package.
2. On the install remote page, enter the Package Location, either an FTP or HTTP server, the file path, and the software package name.
3. Click Fetch and Install Package. The software is activated after the device reboots.

Follow these steps to upload a package from another device to the SRX:

1. Select Maintain > Software > Upload Package.
2. On the upload page, specify the location of the software package on the local system.
3. Click Upload and Install Package. The software is activated after the device reboots.

Uploading Licenses

To enable some Junos features on an SRX, you must purchase, install, and manage separate software licenses.

MORE? For more information about how to purchase software licenses for your device, please visit http://www.juniper.net/generate_license/.

NOTE Before you begin managing licenses in this tutorial, you need to have purchased the license you require and have basic connectivity for the SRX device.

To Add Licenses to Your SRX Device

1. Select the Maintain tab > Licenses as shown in Figure 3.11.

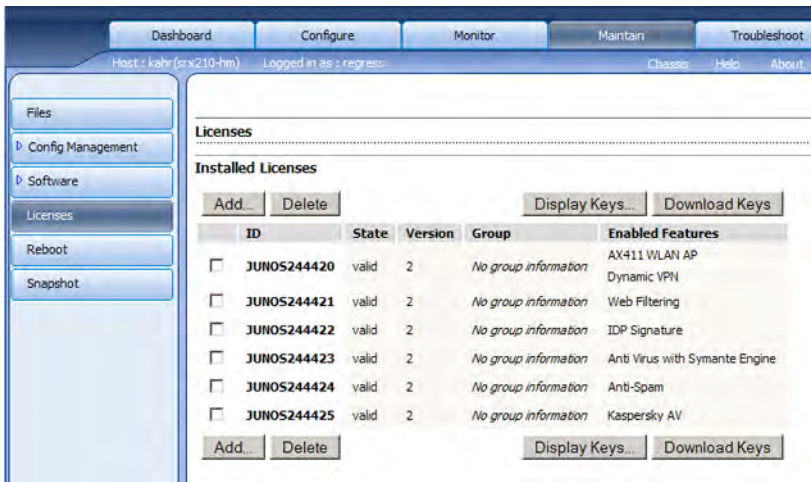


Figure 3.11 Reviewing Your Software Licenses

2. Click the Add button to add a new license key.
3. Complete either Step 4 or Step 5, using a blank line to separate multiple license keys, as shown in Figure 3.12.
4. In the License File URL box, type the full URL to the destination file containing the license key to be added.
5. Or, in the License Key Text box, paste your license key text, in plain-text format, for the license to be added.

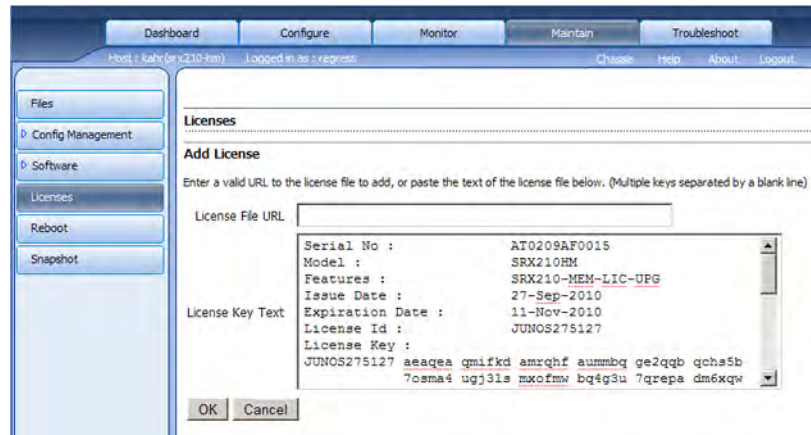


Figure 3.12 Adding the License Text

6. Click OK.
7. Click Commit.

To Delete Licenses from Your SRX Device

1. Select the Maintain tab > Licenses.
2. Select the check box of the license or licenses you want to delete.
3. Click Delete.
4. Click Commit.

To Display License Keys on Your SRX Device

1. Select the Maintain tab > Licenses.
2. Click Display Keys to display all the license keys currently installed.
3. A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.

To Download License Keys Onto the Device

1. Select the Maintain tab > Licenses.
2. Click Download Keys to download all the license keys.
3. Select Save to Disk and specify to which file the license keys are to be written.

Chapter 4

Configuring Device Security

<i>Configuring Interfaces and Zones</i>	<i>50</i>
<i>Configuring Layer 2 Switching</i>	<i>52</i>
<i>Configuring PPPoE</i>	<i>55</i>
<i>Configuring Security Policies.....</i>	<i>58</i>
<i>Configuring Policy Logging.....</i>	<i>60</i>
<i>Configuring Static Routing</i>	<i>61</i>
<i>Configuring NAT.....</i>	<i>62</i>

If you've finished Chapter 3, then you have configured the base system and set up user accounts. Now, you'll learn how to configure a few basic SRX security features such as zones, policies, and NAT.

Keep in mind that you can use the J-Web Configuration Wizards described in Chapter 2, to configure firewall policies, NAT, and VPNs. In fact you might want to check those out first, before attempting to set them up manually. Either way, it's good practice to know both methods of configuring your SRX device.

IMPORTANT Remember that the J-Web options shown in this chapter, and this book, differ depending on the device model, the OS version, and your installed licenses. Use this book's screen captures as guides for what might appear on your device's J-Web interface.

Configuring Interfaces and Zones

Security zones regulate inbound and outbound traffic over an interface by the use of policies, which you define.

You can configure multiple security zones on a single SRX device, but before you do so you must define at least two. You can define security zones with the following tools:

- *Policy*: Defines and enforces rules for all transit traffic, including which packets can pass through the firewall, and any actions the device will impose on that traffic as it passes through the firewall.
- *Screens*: Detect and block various kinds of potentially harmful traffic.
- *Address Books*: Specifies IP addresses and address sets to which you will apply specific security policies.
- *TCP-RST*: Compares arriving traffic with the existing session and sends a RESET flag if the arriving traffic does not match the session and does not set the SYN flag.
- *Interface*: Lists interfaces in a defined zone.

Figure 4.1 shows the Configure tab > Security J-Web page in which you'll do most of your policy work and to which the next few tutorials refer.

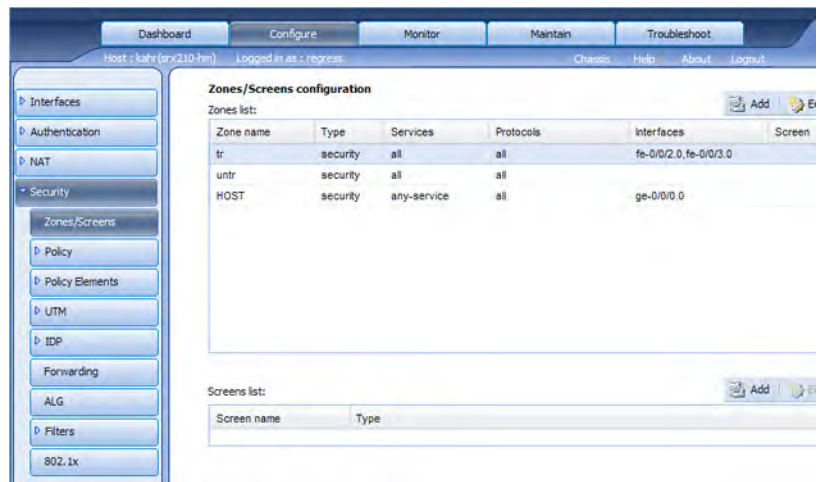


Figure 4.1 Defining Policies in J-Web Using the Configure Tab

To Configure a Zone Using J-Web

1. Select the Configure tab > Security > Zones/Screens.
2. Click the Add button to add a Zone.
3. Set the Zone name.
4. Choose security for the Zone type.
5. Click the Host inbound traffic – Zone tab, and select both Protocols and Services.
6. Click OK.

To Configure an Interface and Assign It to the Security Zone

1. Select the Configure tab > Interfaces.
2. Select the interface you would like to configure and then click Add > Logical Interface.
3. Set Unit to 0.
4. Select the Zone name from the drop-down list.
5. Select the IPv4 Address option.
6. Choose Address/DHCP configuration options and set accordingly.
7. Click OK and then click Commit.

To Configure Address/Address Sets

1. Select the Configure tab > Security > Policy Elements > Address Book.
2. Click the Add button.
3. Select a zone from the Zone name drop-down list .
4. Set the name of the address in the Address Name option.
5. Select either the IP (v4/v6) prefix or Domain Name.
6. Click OK.
7. Click Commit.

Configuring Layer 2 Switching

The lower-end SRX *branch* devices allow you to configure certain Ethernet interfaces to support Layer 2 (L2) switching, in particular, to connect multiple ports to the trust zone in the same L2 domain. Each model of device supports a given set of interfaces that can be used for this purpose, so it's best to check before starting the configuration task. As of Junos 10.2, the allowed interfaces are listed in Table 3.1.

Table 3.1 Configuring SRX Branch Device Ports for Switching

Device	Ports
SRX100 devices	Onboard Fast Ethernet ports (fe-0/0/0 and fe-0/0/7)
SRX210 devices	Onboard Gigabit Ethernet ports (ge-0/0/0 and ge-0/0/1) Onboard Fast Ethernet ports (fe-0/0/2 and fe-0/0/7)
SRX240 devices	Onboard Gigabit Ethernet ports (ge-0/0/0 through ge-0/0/15)
SRX650 devices	Multiport Gigabit Ethernet XPIM modules

On branch SRX devices, the default configuration for Ethernet switching on Fast Ethernet interfaces includes a predefined VLAN named trust, which allows all services and protocols. The default configuration also includes a VLAN interface, vlan.0, which is assigned to the range of predefined interfaces (fe-0/0/0 through fe-0/0/7).

In order to configure Level 2 switching, you'll need to add a VLAN in addition to those that are provided on the SRX device (by default). You will associate some of the interfaces on your system to this new L2 domain, represented by the VLAN.

To Create a New VLAN

1. Select Switching from the left-hand navigation menu.
2. Select VLAN.
3. Click the Add button.
4. Provide a name for your new VLAN as shown in Figure 4.2.

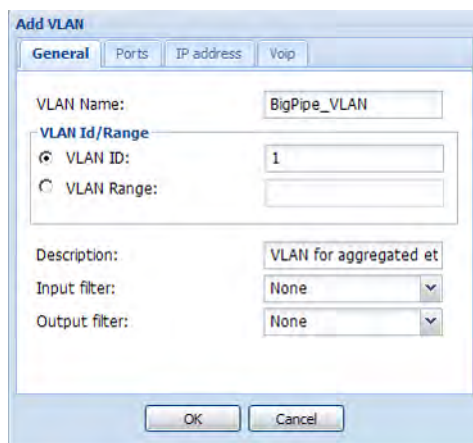
Figure 4.2 Defining a New VLAN

5. Enter an ID number. Do not use a number that has already been used for the default VLANs, for instance, the number 0.

Next, you need to add ports to your VLAN.

To Add Ports to the VLAN

1. Select the Ports tab, as shown in Figure 4.3, which displays a list of the available ports.
2. Select one or more ports to include in your new VLAN.
3. Click OK, and then click OK once more, to close both dialog windows.



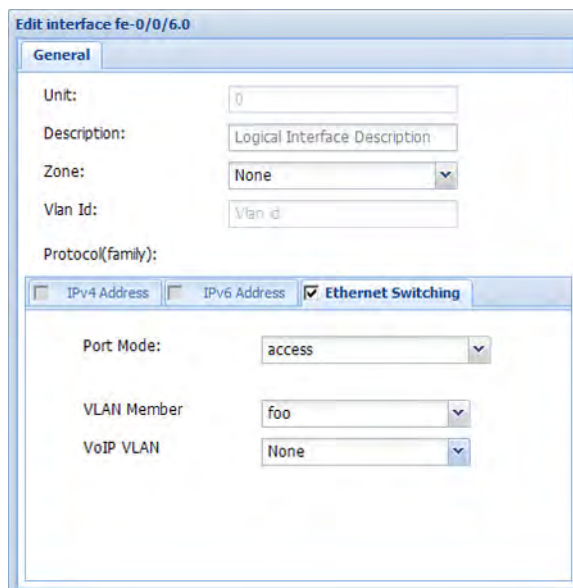
The 'Add VLAN' window in J-Web has four tabs: 'General', 'Ports', 'IP address', and 'Voip'. The 'General' tab is active. It contains the following fields:

- VLAN Name:** A text box containing 'BigPipe_VLAN'.
- VLAN Id/Range:** A section with two radio buttons. The 'VLAN ID' radio button is selected, and its corresponding text box contains '1'. The 'VLAN Range' radio button is unselected, and its text box is empty.
- Description:** A text box containing 'VLAN for aggregated et'.
- Input filter:** A dropdown menu set to 'None'.
- Output filter:** A dropdown menu set to 'None'.

At the bottom of the window are 'OK' and 'Cancel' buttons.

Figure 4.3 Adding Ports to the VLAN

You can now go back to the Configure > Interfaces page and edit each of the interfaces you chose to be included in your new VLAN. You'll see that each logical unit has been created for you and the configuration has been updated to show membership in the new VLAN, as shown in Figure 4.4.



The 'Edit interface fe-0/0/6.0' window in J-Web has a 'General' tab. It contains the following fields:

- Unit:** A text box containing '0'.
- Description:** A text box containing 'Logical Interface Description'.
- Zone:** A dropdown menu set to 'None'.
- Vlan Id:** A text box containing 'Vlan id'.
- Protocol(family):** A section with three radio buttons: 'IPv4 Address' (unselected), 'IPv6 Address' (unselected), and 'Ethernet Switching' (selected).

Below the 'Protocol(family)' section are three more fields:

- Port Mode:** A dropdown menu set to 'access'.
- VLAN Member:** A dropdown menu set to 'foo'.
- VoIP VLAN:** A dropdown menu set to 'None'.

Figure 4.4 Reviewing Interfaces Configured for L2 Switching

Configuring PPPoE

You can configure a PPPoE interface on the branch SRX devices, too. The PPPoE interface helps you create a point-to-point connection between the SRX device and the PPPoE server, otherwise known as an *access concentrator*.

PPPoE is especially useful if your branch office has a DSL connection but you want to take advantage of faster speeds or services that are available from your corporate network, or ISP. For example, you can configure a PPPoE interface that passes traffic to an access concentrator on the service provider broadband network and runs that traffic through a RADIUS authentication server.

Additionally, the DSL line to your branch office might run at 1.5Mbps, while your corporate headquarters' LAN runs at 1Gbps. Using a PPPoE interface, you could continue to use your lower cost DSL line but gain speed advantages on the back-end when connecting to your corporate LAN.

PPPoE interfaces require binding to an underlying Fast Ethernet or Gigabit Ethernet logical interface. Branch SRX devices include a logical interface called *pp0*, which you can configure as your PPPoE interface.

To Configure a PPPoE Interface

1. Open the Configure tab > Interfaces. Then select the pp0 row in the table of interfaces in J-Web as shown in Figure 4.5.

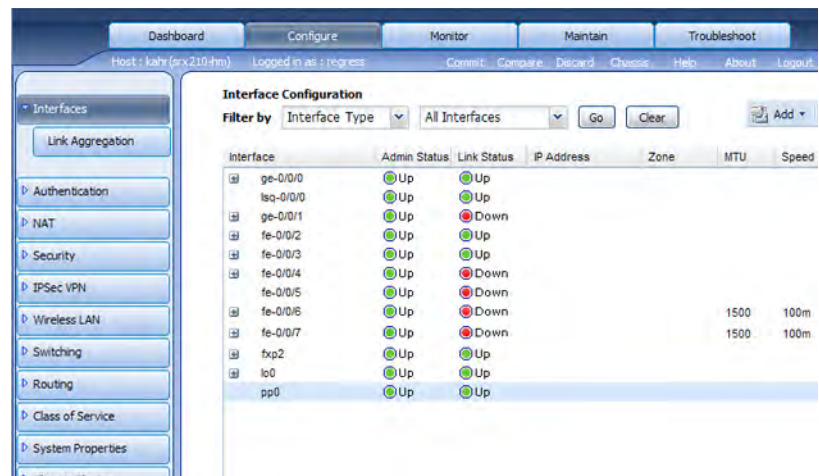


Figure 4.5 Selecting the pp0 Interface

2. Click Edit.
3. Enter the PPOE description; this is optional, but doing so makes it easier to keep track of.
4. Enter the IP address for the logical interface as shown in Figure 4.6. You need to enter a prefix or the entire IPv4 address, plus a netmask value, for example: 10.10/8 or 10.10.10.0/8

Figure 4.6 Configuring the PPPoE Interface

5. Enter the access concentrator name as shown in Figure 4.6. You may need to ask your ISP or IT administrator for the name/location of the concentrator.
6. Select the underlying interface from the list of available interfaces as shown in the detail of Figure 4.7. For most branch devices, you must select either a Fast Ethernet or a Gigabit Ethernet interface.

Figure 4.7 shows the 'PPPoE Options' dialog box. It contains the following fields and values:

Field	Value
Access Concentrator	isp.access.com
Auto Reconnect Time	
Idle Timeout	
Service Name	
Underlying Interface	fe-0/0/3.0

Figure 4.7 Setting the pp0 Underlying Interface

7. Click OK.
8. Click Commit.

If a dialog box appears that shows an “Interface Not Found” message under the Link State column, as shown in Figure 4.8, you probably need to configure the interface you selected as the underlying interface (shown previously in Figure 4.7).

Figure 4.8 shows the 'Configure Interfaces' dialog box. The 'Logical Interfaces' table is as follows:

Logical Interface Name	Link State	Configured	Description
pp0.0	Interface Not Found	Yes	PPPoE RADIUS

The 'Physical Interface Description' field is empty.

Figure 4.8 Reviewing PPPoE Logical and Physical Interfaces

And, if you run into problems with the commit, review the configuration in the CLI Editor:

1. Select CLI Tools from the left-hand navigation menu.
2. Select CLI Editor.
3. Scroll down to find your pp0 interface and the underlying interface.

Sometimes, you may have a logical unit that is already defined as an *inet family*, which is incompatible with PPPoE. If that’s the case, you can directly edit your configuration file in the CLI Editor, as shown in Figure 4.9, by selecting CLI Tools> CLI Editor. After making changes, don’t forget to click Commit.

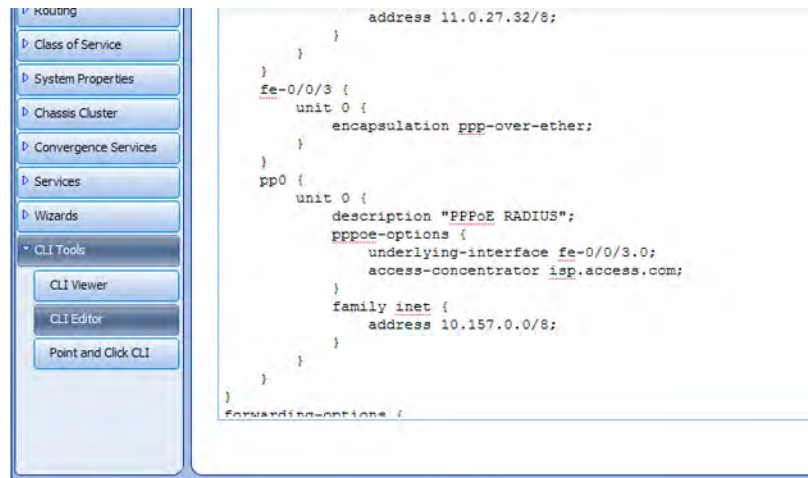


Figure 4.9 Fixing Interface Configurations in the CLI Editor

Configuring Security Policies

Policies enforce rules for transit traffic – packets enter one security zone and exit through another security zone. Policies allow you to deny, permit, reject, authenticate, and perform many other operations on the transiting traffic.

Right out of the box, the SRX device denies all traffic in all directions as a security measure. By denying all traffic at this initial stage, you can securely connect your new device without concern that it may be the target of some type of attack before you are able to properly configure it.

To allow data traffic to pass between zones, you must first configure security policies. Every policy has five characteristics:

- *Direction*: an incoming zone to an outgoing zone (from-zone to to-zone).
- *Source address name*: One or many names or source address set names.
- *Destination address names*: One or many names or destination address set names.
- *Application name*: One or many names or application set names.

- **Action:** An action to perform on a defined address name, address name, application, or application set name.

Before you begin the process of defining a policy, you should complete the following tasks:

- Establish basic connectivity.
- Configure security zones and interfaces (see *Configuring Zones and Interfaces* earlier in this chapter).
- Configure address books (see *Configuring Zones and Interfaces* earlier in this chapter).

To Configure a Policy on Your SRX Device

1. Select the Configure tab > Security > Policy > FW Policies.
2. Click the Add button to add a policy and you'll see a screen similar to Figure 4.10, to which Steps 3-9 refer.

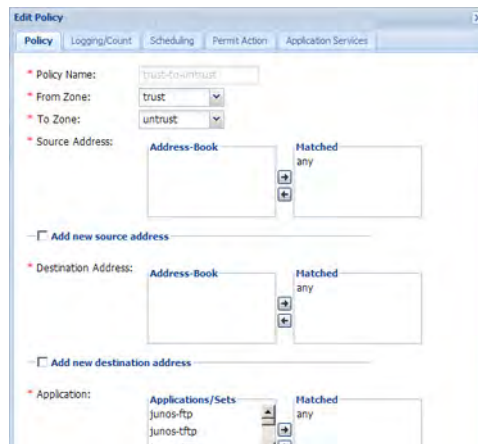


Figure 4.10 Configuring and Editing a Security Policy

3. Enter the Policy Name.
4. From the Policy Action drop-down list, select permitted, denied, or rejected to specify how matching traffic will be handled.
5. Select the source zone from the From Zone drop-down list.
6. Select the destination zone from the To Zone drop-down list.
7. Select the required action from the Policy Action drop-down list.

8. Specify the source address for the policy by selecting the appropriate Source Address options. If the address is a new address, select the Add new source address checkbox and enter the IP address and name.
9. Specify the destination address for the policy by selecting the appropriate Destination Address options. If the address is new, select the Add new destination address checkbox and enter the IP address and name.
9. Specify the name of the application or application set to which the policy applies by selecting the appropriate Applications options.
10. Click OK.
11. Click Commit.

Configuring Policy Logging

Setting up policy logging is critical to tracking the security of your traffic. Policy logs allow you to monitor general traffic based on the policies you define, as well as specific conditions and IP addresses.

To Configure Policy Logging

From either the Edit Policy dialog, or the Add Policy dialog as shown in Figure 4.11, you can easily configure policy logging.

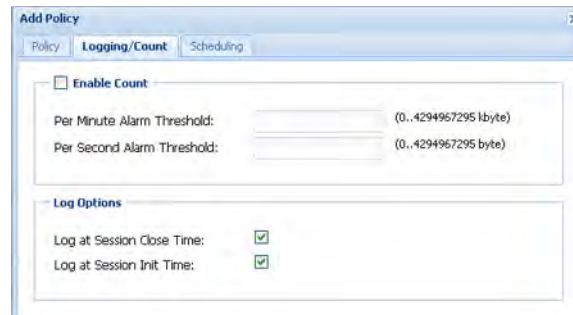


Figure 4.11 Configuring Policy Logging Options

1. Click the Logging/Count tab.
2. Select the Log at Session Close Time option.

3. Select the Log at Session Init Time option.
4. Click OK.
5. Click Commit.

You can now view policy logs from the Maintain Files page in J-Web.

Configuring Static Routing

Static routing enables you to control the traffic path and destination, once traffic leaves the current device. By deploying static routing, particularly in a network with only one outbound path, you can decrease the overhead on the network. In J-Web, you configure static routing within the Configure tab options, as shown in Figure 4.12.

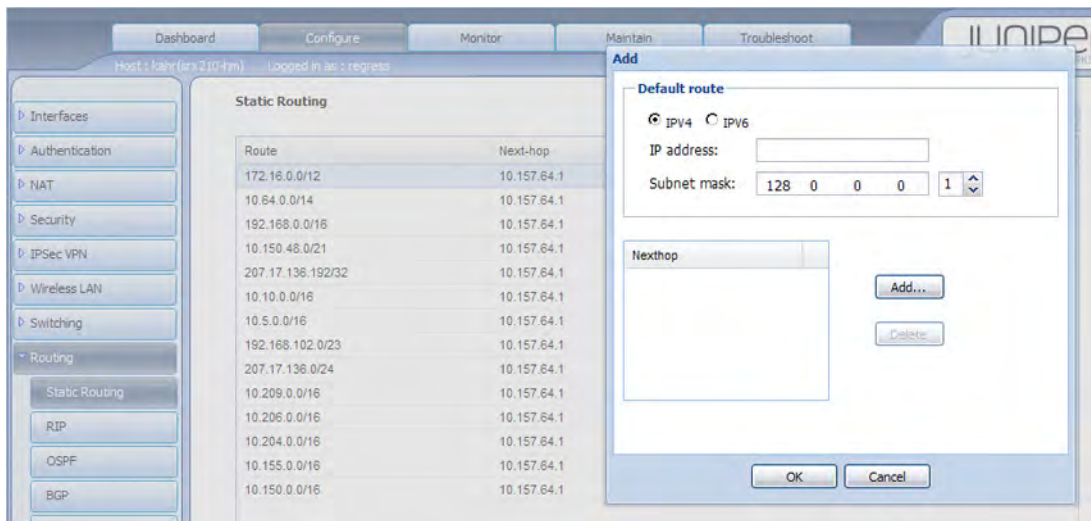


Figure 4.12 Configuring Static Routing Options

To Configure Static Routing on Your SRX Device

1. Select the Configure tab > Routing > Static Routing.
2. Click Add to add a static route.
3. Select IPv4 or IPv6 and Subnet mask as shown in Figure 4.13.

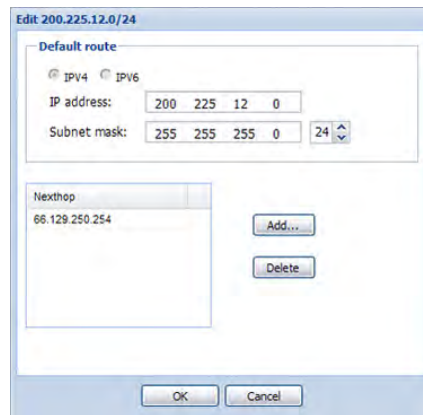


Figure 4.13 Configuring the IP Address and Nexthop

4. Add the Nexthop address.
5. Click OK and then click Commit.

Configuring NAT

Network Address Translation (NAT) allows you to hide an entire private address space behind a single public IP address. Using a translation table on the device, source and destination addresses can be translated into known addresses that shield the original packet header address from scrutiny on the Internet. The NAT address that the device applies to any source and destination addresses is viewed as a single gateway address.

NAT often includes the translation of port numbers as well as IP addresses.

NOTE You can also perform configuration of source, destination, and static NAT using the J-Web NAT Configuration Wizard, described in detail in Chapter 2.

Your SRX device supports three different types of NAT:

- *Source NAT* allows you to change the source address, so that subsequent devices cannot determine the origination address.
- *Destination NAT* allows you to change the destination address. Destination NAT is useful for port forwarding and other types of translation.

- *Static NAT* allows you to establish a one-to-one mapping between a public and a private address. Typically, you use static NAT to enable a connection to your private network from a public network.

To enable NAT, you'll need to set up rules and rule sets, to which NAT compares a given IP address until it finds a match. Once NAT finds a match, it applies the corresponding rule. For example, a rule set can match traffic from a specified interface or zone.

NAT address pools allow you to configure a set of addresses from which NAT can choose when applying addresses to source or destination addresses. This can be useful for a number of reasons, including load balancing.

For example, you can set up an address pool in which each address in the pool points to a different internal web server. You can route incoming Internet traffic to the address pool, and NAT will assign one of the addresses to that incoming address, allowing for a more evenly distributed load on your web servers.

To define source NAT address pools, you'll need to specify the following on your SRX device, so you can enter the information in the Configuration tab's NAT options as shown in Figure 4.14 (next page):

- Name of the source NAT address pool.
- Address or address ranges.
- Routing instance to which the pool belongs (the default is the main inet.0 routing instance).
- No port translation (optional). By default, port address translation is performed with source NAT.

ALERT! Do not overlap NAT addresses for source NAT, destination NAT, and static NAT within one routing instance.

To Configure a Source NAT Pool on Your SRX Device

1. Select the Configure tab > NAT > Source NAT.
2. Select the Source NAT Pool tab.
3. Click Add to add a new NAT pool.
4. Enter the Pool Name.
5. Add Pool Addresses or an Address Range.

6. Choose the required Port Translation option.
7. Click OK and then click Commit.

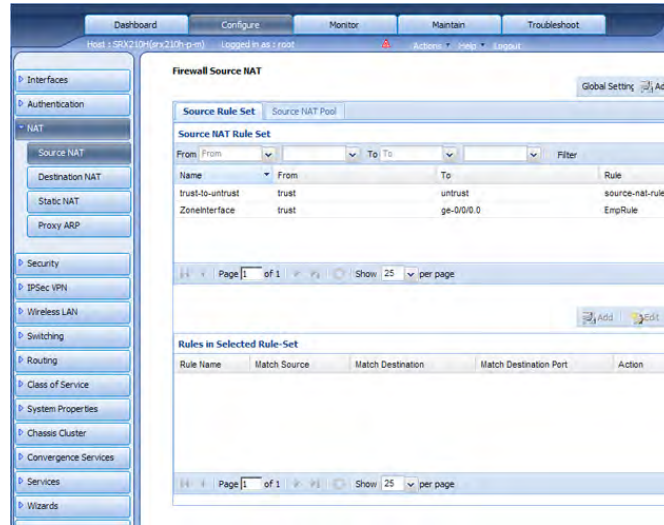


Figure 4.14 Configuring the Source NAT Option

To Configure a Source NAT Rule Set

1. Select the Configure tab > NAT > Source NAT and then select the Source Rule Set tab.
2. Click Add to add a new Rule Set.
3. Enter the Rule Set Name.
4. Use the From drop-down list to specify the source.
5. Use the To drop-down list to specify the destination.
6. Click Add to add a new rule.
7. Enter the Rule Name and the Source and Destination addresses.
8. Select the desired Action to be performed.
9. Click OK and then click Commit.

MORE? If you need more information about any of these features, see: *Day One: Deploying SRX Series Services Gateways* at www.juniper.net/dayone; *Junos Security*, by Cameron, et. al., published by O'Reilly Media, at www.juniper.net/books; or, consult the SRX device documentation at www.juniper.net/techpubs.

Chapter 5

Monitoring with J-Web

<i>Monitoring Events and Alarms</i>	<i>66</i>
<i>Viewing System Events</i>	<i>67</i>
<i>Monitoring the Chassis</i>	<i>69</i>
<i>Monitoring Interfaces</i>	<i>70</i>
<i>Monitoring Source NAT</i>	<i>71</i>
<i>Monitoring Sessions</i>	<i>72</i>

This chapter shows you how to use J-Web to monitor some of the basic elements on your SRX device, such as chassis alarms, system events, NAT, and DHCP. The J-Web Dashboard includes a number of static and dynamic displays where you can quickly find statistics and graphs about the general health of your device, your configuration, and traffic patterns.

As with every chapter in this book, this chapter assumes you're following along on a testbed or an actual SRX device, which means you have already configured some basic services.

IMPORTANT Remember that the J-Web options shown in this chapter, and this book, differ depending on the device model, the OS version, and your installed licenses. Use this book's screen captures as guides for what might appear on your device's J-Web interface.

Let's start by checking the chassis alarms to make sure that everything is running as you expect it to run.

Monitoring Events and Alarms

You can quickly monitor both your system and chassis alarms using J-Web. System alarms are fairly easy to figure out. In fact, the system alarms consist of predefined messages indicating that you have not yet committed a rescue configuration, or maybe you neglected to install a required software license.

Chassis alarms are those predefined alarms that show up as colored lights on the front of the device. Chassis alarms typically indicate a problem with the environment (temperature, fan state) or with the interface PIM (in the SRX device, the flexible port concentrator (FPC), and the PIM are the same thing).

To Monitor Your System and Chassis Alarms

1. Select the Monitor tab as shown in Figure 5.1.
2. Select Events and Alarms > View Alarms.

J-Web displays a list of the alarms in the bottom panel. Each alarm is time-stamped. (If you want to filter the alarms, choose the alarm type, severity, a description, or a date range from the Alarm Filter section.)

EXPLORE Try some different variation of alarm, descriptions, and severities on your own SRX if you're following along. Having a full suite of helpful alarms can prevent larger issues down the line.

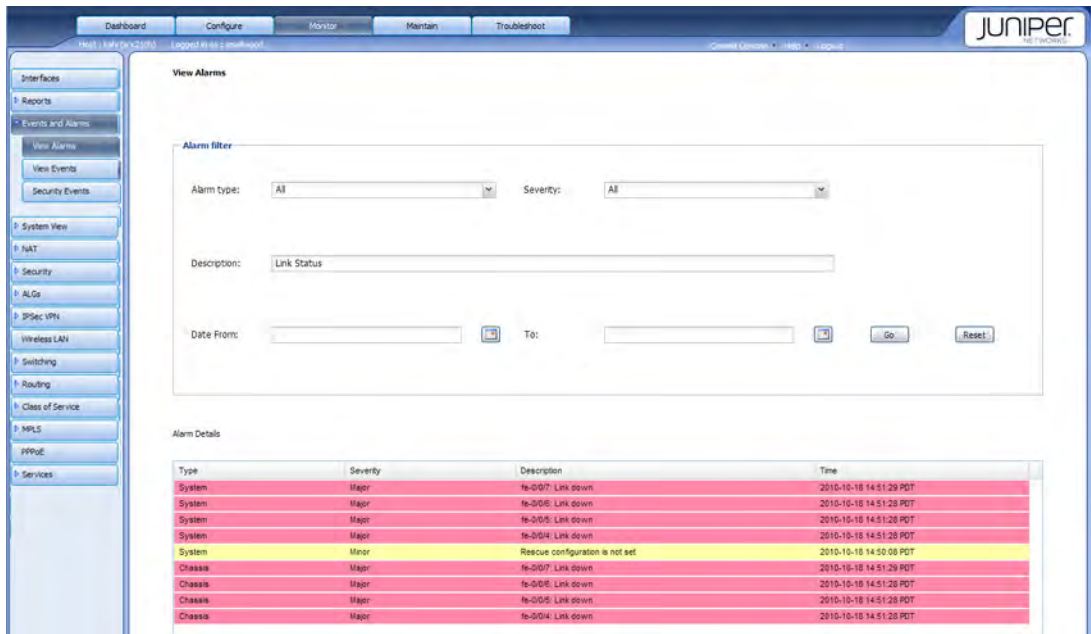


Figure 5.1 Monitoring Events and Alarms

Viewing System Events

System events are a broader category than system and chassis alarms.

The Junos system log file contains details about every event that occurs on your device, including, but not limited to, actions and operations you perform using J-Web, authentication events, login and logout events, and many more. In the event message display, the messages are color-coded by type, as indicated in the color-code legend at the bottom of the Events Detail pane. Typically, the most common events are the green informational event messages.

NOTE

If you happen to set the Ethernet Link Down alarm and you don't yet have your Ethernet interface configured, you may see a list of alarms highlighted in pink, showing the critical message that your links are down for your ge-0/0/1 interface and possibly your fe interfaces.

Back in Chapter 3 you should have configured SNMP and the SNMP-Health alarm, so now you can find the event messages on the View Events page as shown in Figure 5.2.

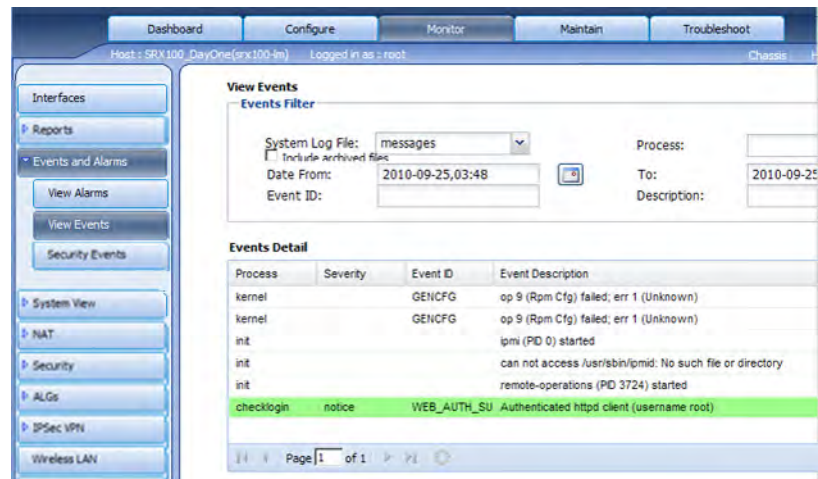


Figure 5.2 Monitoring Events in J-Web

To View System Events

1. Select the Monitor tab.
2. Select Events and Alarms > View Events.
3. At a minimum, choose the System Log File: either the messages file, or security file.
4. You can filter events by entering a Process Name, an Event ID, a Description, or a Date range in the Events Filter pane.
5. If you want to include archived system logs, check the Include archived files option. Selecting this option can increase the time required to display results and can cause a performance hit, if there are many archived files.
6. Click the Generate Report button to create an HTML report of the events.

J-Web displays a list of the events in the bottom pane. Each event is time stamped and the process or daemon that generated the message is listed. Other properties can include the severity, event ID, and a description. Some of these are previously shown in Figure 5.2.

Monitoring the Chassis

While the J-Web Dashboard provides a quick view into the health and resource utilization of your SRX device, you may want to dig deeper when monitoring the chassis.

The System View provides details on the hardware system, including part and serial numbers, routing engine details, CPU usage, temperature, power supply status, and more as shown in Figure 5.3.

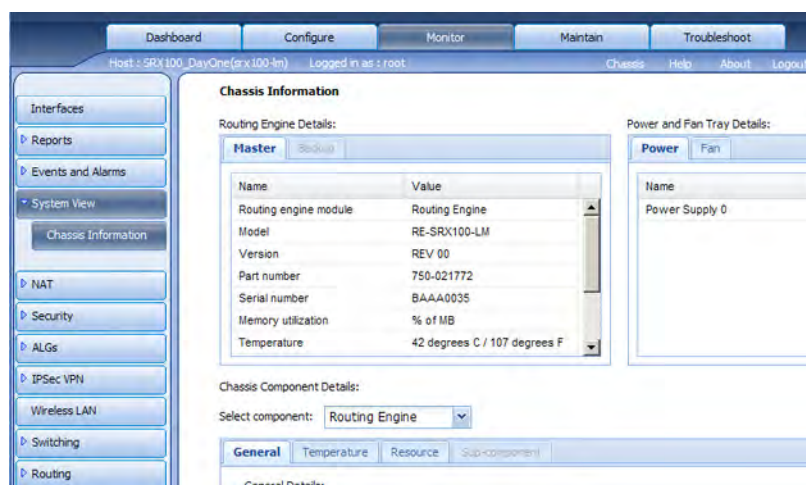


Figure 5.3 Reviewing Chassis Statistics in J-Web

To View Basic Master Chassis Information

1. Select the Monitor tab.
2. Select System View > Chassis Information.
3. By default, details are shown for the routing engine in the Chassis Component Details pane.
4. Select the Temperature tab to view the chassis and CPU temperatures.
5. Select the Resource tab to see how much CPU DRAM is being used.
6. To view details about any PIMs you have installed in the SRX device, select FPC 0 from the Select component drop-down menu.

Monitoring Interfaces

J-Web gives you a quick view of the available ports right on the home Dashboard page (click the Dashboard tab). Hover your mouse pointer over one of the ports on the graphical view of the router on the Dashboard.

TIP Right-click to see a menu that lets you navigate right to the Configuration or Monitoring page for that port.

For a more detailed view, select the Monitor tab. By default, the first display you see is the Interfaces page. Right at the top of the page, you can see a list of the available ports, their state, and a few other statistics as shown in Figure 5.4.

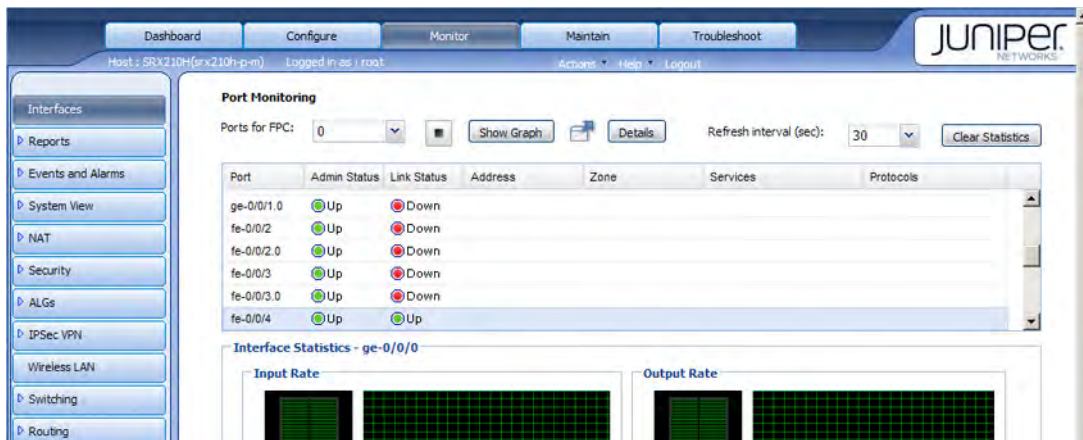


Figure 5.4 Monitoring Interface Statistics

To Drill Down to See All of the Statistics for a Given Port

1. Select a port from the list.
2. Click the Details button at the top of the page. A separate window appears that contains all General, Traffic, and Address details.

Monitoring Source NAT

J-Web enables you to monitor everything that you might configure. Explore it endlessly. However, at this point let's just make sure the major services you've configured are up and running. Most likely, you have configured NAT (as instructed in Chapter 4), and now you need to perform some quick monitoring to see if it is operating as planned.

Whenever monitoring NAT, you may first be interested in viewing the number of translation hits.

To Monitor NAT Using J-Web

1. Select the Monitor tab.
2. Select NAT > Source NAT. (For the most part, by default, under the Rules tab, J-Web displays information that you defined, such as the interface names and IP pool addresses.)
3. Scroll to the bottom of the page to see the top 10 translation hits (depending on your test device or test bed, there could be little or a lot of information). You can see this statistic for destination and static NAT as well, as shown in Figure 5.5.

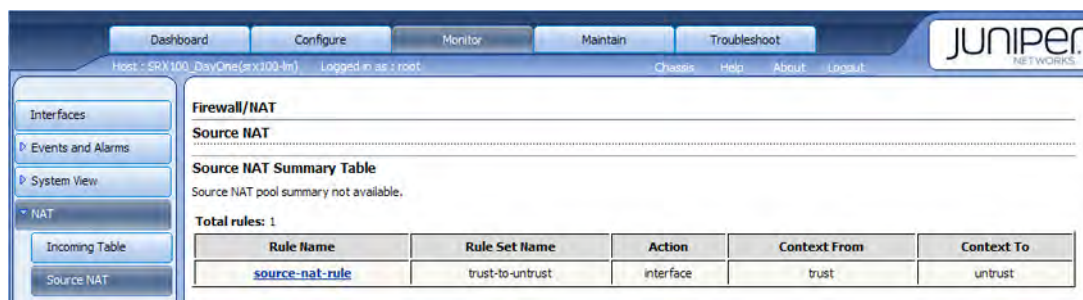


Figure 5.5 Monitoring Source NAT in J-Web.

You can define NAT rules for different ports. For example, for email traffic, you might set a low timeout value or even take the default of 60 seconds (on an SRX210H device). In that case, the device flushes your translation table frequently, and the monitoring page may show a high number of timeouts for that ruleset.

On the other hand, if you configure one of your interfaces to specifically manage FTP traffic, you may want to define a longer timeout

value, as an FTP session often experiences long periods of inactivity. In that case, the timeout value for that ruleset will be low. However, if you note a high number of timeouts on the FTP port, you may want to investigate.

Monitoring Sessions

By default, the branch SRX devices (SRX100, SRX210, SRX240, and the SRX650) save all syslog messages in a file called, appropriately enough, messages. You can create your own log files, but the messages file will contain plenty of information for you to get started.

How to Look at the Messages File

1. Click the Maintain tab.
2. Click the Files button in the left-side navigation menu.
3. Under the section titled, “Download and Delete Files,” click the “Log Files” link.
4. Scrolling down the list of files, locate the messages file. You may find some gzipped messages files as well. These are compressed archived log files.
5. Click the “Download” link to download the messages file to your locally connected device (your PC).
6. Open the file in a simple text editor to view the messages, as shown in Figure 5.6 (opened on a Mac).

NOTE By default, the SRX devices in the branch family begin a new messages file once the current file reaches 100K in size. The messages file contains every event that occurs during the operation of the SRX device.

How to Create your Own Syslog Files.

The easiest way to create your own syslog files is to use the Point and Click CLI Editor.

1. Click the Configure tab.
2. Click the CLI Tools link in the navigation menu.
3. Click Point and Click CLI as shown in Figure 5.7.

```

Sep 25 06:00:16 SRX100_DayOne newsyslog[1050]: logfile turned over due to size=100K
Sep 25 06:00:41 SRX100_DayOne srarpd[1944]: SNMPD_TRAP_COLD_START: trap.generate_cold: SNMP trap: cold start
Sep 25 06:01:16 SRX100_DayOne /kernel: GENCFG: op 2 (GenCfg Blob) failed; err 7 (doesn't Exist)
Sep 25 06:01:22 SRX100_DayOne /kernel: GENCFG: op 3 (GenCfg Blob) failed; err 7 (doesn't Exist)
Sep 25 06:01:25 SRX100_DayOne /kernel: GENCFG: op 9 (Ppe Cfg) failed; err 1 (Unknown)
Sep 25 06:01:29 SRX100_DayOne init: can not access /usr/sbin/ipmid: No such file or directory
Sep 25 06:01:29 SRX100_DayOne init: ipmi (PID 8) started
Sep 25 06:10:46 SRX100_DayOne login: LOGIN_INFORMATION: User root logged in from host [unknown] on device ttyu0
Sep 25 06:10:46 SRX100_DayOne login: LOGIN_ROOT: User root logged in as root from host [unknown] on device ttyu0
Sep 25 06:13:25 SRX100_DayOne checklogin[1137]: WEB_AUTH_SUCCESS: Authenticated httpd client (username root)
Sep 25 10:40:42 SRX100_DayOne /kernel: getnewslog: nsgbufp[size=32768] = 0x0000cfef
Sep 25 10:40:42 SRX100_DayOne /kernel: Copyright (c) 1995-2010, Juniper Networks, Inc.
Sep 25 10:40:42 SRX100_DayOne /kernel: All rights reserved.
Sep 25 10:40:42 SRX100_DayOne /kernel: Copyright (c) 1992-2006 The FreeBSD Project.
Sep 25 10:40:42 SRX100_DayOne /kernel: Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
Sep 25 10:40:42 SRX100_DayOne /kernel: The Regents of the University of California. All rights reserved.
Sep 25 10:40:42 SRX100_DayOne /kernel: JUNOS 10.1R1.8 #0: 2010-02-12 10:31:54 UTC
Sep 25 10:40:42 SRX100_DayOne /kernel: builder@queth.juniper.net:/volume/build/junos/10.1/release/10.1R1.8/obj-ocetson/bsd/sys/compile/3SRONLE
Sep 25 10:40:42 SRX100_DayOne /kernel: JUNOS 10.1R1.8 #0: 2010-02-12 10:31:54 UTC
Sep 25 10:40:42 SRX100_DayOne /kernel: builder@queth.juniper.net:/volume/build/junos/10.1/release/10.1R1.8/obj-ocetson/bsd/sys/compile/3SRONLE
Sep 25 10:40:42 SRX100_DayOne /kernel: real memory = 536870912 (512MB)
Sep 25 10:40:42 SRX100_DayOne /kernel: avail memory = 313733120 (299MB)
Sep 25 10:40:42 SRX100_DayOne /kernel: cpuid: 0, btb_cpupack:0xffffffff
Sep 25 10:40:42 SRX100_DayOne /kernel: FreeBSD/SMP: Multiprocessor System Detected: 2 CPUs
Sep 25 10:40:42 SRX100_DayOne /kernel: Initializing watchdog interrupt
Sep 25 10:40:42 SRX100_DayOne /kernel:
Sep 25 10:40:42 SRX100_DayOne /kernel: Loading RT Fifo module.....
Sep 25 10:40:42 SRX100_DayOne /kernel: Loaded RT Fifo module
Sep 25 10:40:42 SRX100_DayOne /kernel: pmap_helper loaded (interface version 6, bsyscall 210)
Sep 25 10:40:42 SRX100_DayOne /kernel: cpu0 on motherboard

```

Figure 5.6 Reviewing Session Logs

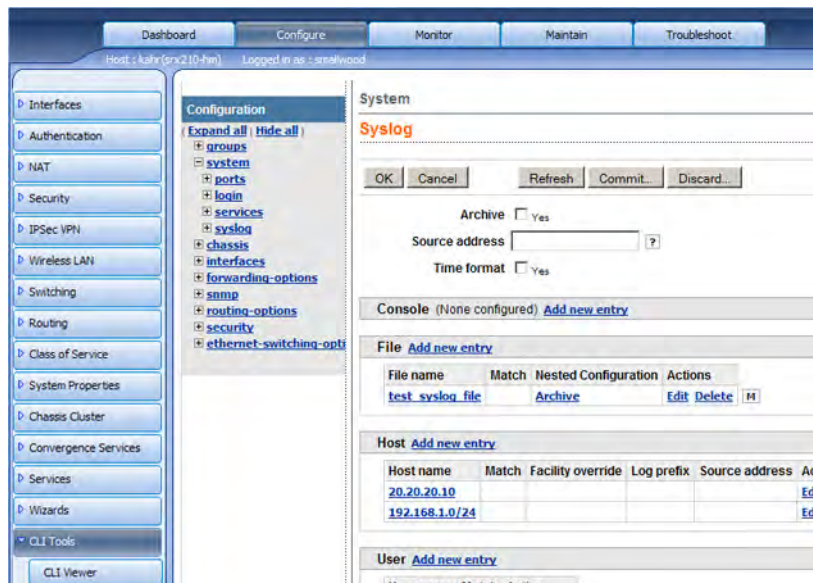


Figure 5.7 Configuring Syslog Files in the Point and Click CLI

4. Click the System > Configure link.
5. Click the Syslog > Configure link.

6. Choose the Syslog elements you want to configure as shown in Figure 5.8.

System

Syslog

OK Cancel Refresh Commit Discard

Archive ☐ Yes
Source address
Time format ☐ Yes

Console (None configured) [Add new entry](#)

File (None configured) [Add new entry](#)

Host [Add new entry](#)

Host name	Match	Facility override	Log prefix	Source address	Actions
20.20.20.10					Edit Delete

User [Add new entry](#)

User name	Match	Actions
*		Edit Delete

Advanced

OK Cancel Refresh Commit Discard

Icon Legend

- Comment: The configuration statement has been annotated with a comment. To display the comment, place the cursor over the statement icon.
- Inactive: The configuration statement is not active and does not affect the device.
- Modified: The configuration statement has been changed or added.

Desktop My Documents Search Desktop 97%

Figure 5.8 Setting Syslog Configuration Parameters

7. When you're done, be sure to click OK, and then click Commit.

MORE? For more details about Junos system log messages, refer to the Junos System Log Messages Reference for the release currently installed, available at www.juniper.net/techpubs/software/junos/index.html (click on the References section of Junos documentation).

Chapter 6

Diagnosing Network Problems

<i>Checking Connectivity with Ping Host</i>	<i>77</i>
<i>Practice: Solving Path MTU Problems</i>	<i>80</i>
<i>Practice: Identifying Hosts with Traceroute</i>	<i>83</i>
<i>Summary</i>	<i>86</i>

This chapter shows you how to use J-Web's diagnostic tools to troubleshoot routing and security problems. Although the tools are easy to use with the J-Web interface, you can discover complex details about your traffic and packet flow. So don't let the ease of these tutorials fool you – learning how to read J-Web's diagnostic tools like Ping and Traceroute can make the difference between just identifying a problem and actually solving the problem. This chapter specifically describes:

- Ping Host
- Traceroute
- Packet Capture

EXPLORE

There are several other troubleshooting tools in J-Web that you'll want to explore on your own, or in between reading sections of this chapter:

- **Ping MPLS:** This tool tests connectivity to Label-Switched Paths (LSPs), L2 and L3 VPNs, and L2 circuits.
- **RPM:** Helps you set up and view real-time performance monitoring (RPM) probes.
- **CLI Terminal:** Allows you to issue router operational and configuration commands, as well as typical UNIX commands by way of a Java applet embedded in J-Web.

You can easily locate the troubleshooting tools that are integrated into the J-Web interface by selecting the Troubleshoot tab from the J-Web menu tabs. Selecting the Troubleshoot tab displays the Ping Host page, along with the other troubleshooting tools as shown in Figure 6.1.

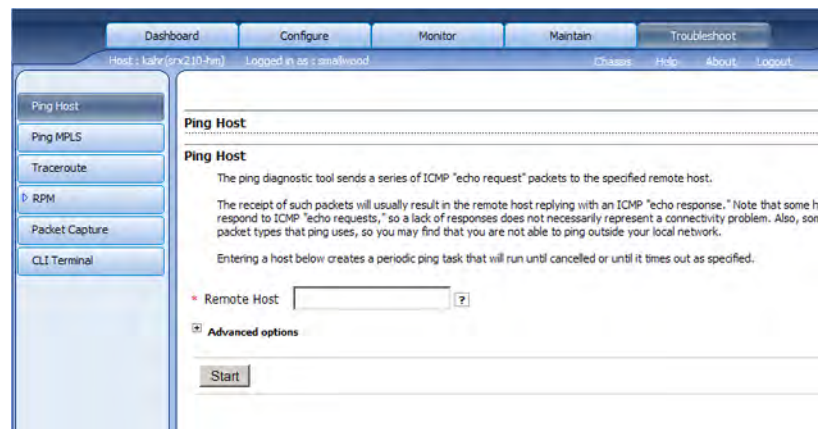


Figure 6.1 Reviewing the Main Troubleshooting Page

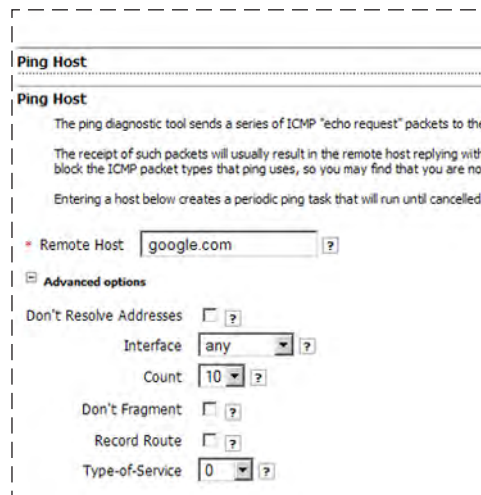
Checking Connectivity with Ping Host

The packet internet groper command, or Ping, is an incredibly simple tool that provides powerful results. You can easily use Ping to test your connectivity to a specific server. Default Ping output is fairly easy to understand. But the J-Web UI provides you a much more powerful set of Ping capabilities. For example, you can diagnose several common connectivity problems, including path MTU problems, by correctly interpreting Ping output, and that's where J-Web comes in.

NOTE When running Ping, you can specify either the IP address or the hostname (if you know it). If you specify the hostname, Ping will resolve the hostname to its IP address by default.

Test for Basic Connectivity to Another Device

1. Start at the Ping page in the J-Web interface.
2. Enter the Hostname or IP address in the Remote Host field as shown in Figure 6.2.
3. Click Start.



The screenshot shows the 'Ping Host' interface in the J-Web UI. It includes a title bar 'Ping Host', a description of the ping diagnostic tool, and a form for entering host information. The 'Remote Host' field is set to 'google.com'. Below this, there is an 'Advanced options' section with several checkboxes and dropdown menus: 'Don't Resolve Addresses' (unchecked), 'Interface' (set to 'any'), 'Count' (set to '10'), 'Don't Fragment' (unchecked), 'Record Route' (unchecked), and 'Type-of-Service' (set to '0'). Each field has a help icon (?) next to it.

Figure 6.2 Entering Ping Host Query Parameters

That's all there is to it. If you don't specify any advanced options, the results you get may be limited, but sometimes you only need to see if you can communicate with another host or device. The output shown

in Figure 6.3 is the result of a Ping command. Typically, if you cannot connect to the host, Ping will return a request timed out ICMP error message.

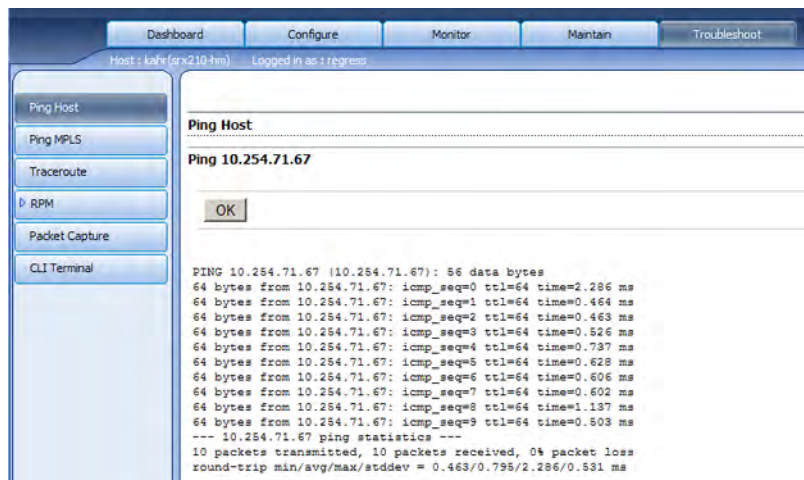


Figure 6.3 Reviewing Ping Results

If all you want to do is test connectivity between two directly connected devices, simply using Ping is often enough to help you resolve the problem. However, with the complexity of networks today, it's unlikely that many of your connectivity problems will be this simple, so let's get more advanced.

By clicking the small plus (+) icon next to the Advanced options label, just below the Remote Host field, as shown in Figure 6.2, you can view and modify a host of advanced Ping options. In a number of specific cases, you can use different options to reveal information that can help you track down and solve routing problems.

EXPLORE Take a moment and wander through some of the Ping options in J-Web. If connected to a test bed or a real network, test a few out. It's so simple and fast that exploring Ping can teach you quickly how powerful this one J-Web tool can be.

MORE? You can find a complete list of advanced Ping options in the *Junos Security Administration Guide* at: <http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-admin-guide/index.html>

To Solve Interface Configuration Problems

If you suspect that your connectivity issues are a result of a misconfigured interface, you can run your Ping request over a specific interface. By default, Ping issues requests over *any* available interface, which makes it difficult to diagnose the interfaces. If you specify your Ping requests over a specific interface, and Ping returns no results, it's very possible that you have a problem with that interface.

Figure 6.4 shows an example of how to run Ping over only the ge-0/0/0 interface on an SRX device, and Figure 6.5 details the Ping results received from the Ping request of Figure 6.4.

Ping Host

The ping diagnostic tool sends a series of ICMP "echo request" packets to the specified remote host.

The receipt of such packets will usually result in the remote host replying with an ICMP "echo response." Note that some hosts are configured not to respond to ICMP "echo requests" connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you may find that you are not able to ping outside your local network.

Entering a host below creates a periodic ping task that will run until cancelled or until it times out as specified.

Remote Host:

Advanced options

Don't Resolve Addresses: ☒

Interface:

Count:

Don't Fragment: ☐

Record Route: ☒

Type-of-Service:

Routing Instance:

Interval:

Packet Size:

Source Address:

Time-to-Live:

Bypass Routing: ☐

Start

Figure 6.4 Specifying a Ping Over a Specific Interface

Ping Host

Ping 172.23.7.32

OK

```
PING 172.23.7.32 (172.23.7.32): 56 data bytes
64 bytes from 172.23.7.32: icmp_seq=0 ttl=122 time=155.256 ms
RR:
10.149.0.66
172.24.19.12
172.24.19.2
172.24.193.66
10.187.71.67
172.23.7.32
172.24.193.70
172.24.230.90
172.24.19.2
64 bytes from 172.23.7.32: icmp_seq=1 ttl=122 time=144.254 ms (same route)
64 bytes from 172.23.7.32: icmp_seq=2 ttl=122 time=129.496 ms (same route)
64 bytes from 172.23.7.32: icmp_seq=3 ttl=122 time=208.038 ms (same route)
--- 172.23.7.32 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max/stddev = 129.496/159.261/208.038/29.607 ms
```

Figure 6.5 Reviewing Results of a Ping over the ge-0/0/0 Interface

Practice: Solving Path MTU Problems

Up until now, this book has shown individual solutions to some common configurations on the SRX. Now let's focus on a small case study to put J-Web to the test. Obviously it's an easy case study, but the idea is to jog your brain into thinking multi-functionally with J-Web.

Both the Ping Host command and the Traceroute command can help you determine packet length suitability. You might be wondering why this is something you should even worry about. The answer is fragmentation.

The Internet Protocol (IP) can fragment and defragment packets that are too large. Generally, if your source and destination hosts are connected directly, you won't need to worry much about fragmentation, because you can easily determine and define compatible maximum transmission unit (MTU) sizes for your egress and ingress interfaces.

If you use the Internet as a transmission medium between LANs, however, you may find it nearly impossible to control the acceptable packet size. If you send a packet that's 1500 bytes long (MTU default) and that packet is routed to a device that has an MTU value of 576, that device is going to break your packet into three or more fragments, include copies of header tags in those fragments, and pass them along to the next hop.

Eliminating Fragmentation

If you don't allow fragmentation of your packets (by setting the DF, or Don't Fragment option) then the intermediate device whose MTU is 576 will reject your packet and send an ICMP error message back to your router. You can then decide how you want to handle the traffic to that destination. If you don't care whether or not your packets are fragmented, you can set the device to adjust the MTU for that destination in the route table and resend a smaller packet. Or you might configure the device to try another path.

The Costs of Fragmentation

Unfortunately, many new types of transmitted data, like streaming video, or teleconferenced voice, don't tolerate fragmented packets as well as simpler data formats like email messages or text files. Additionally, if your data is time-sensitive, or your terms of service vary, you

may not want your data to be shuttled back and forth in the hopes that you'll find a path with a compatible MTU.

Another problem with fragmentation is the processing overhead associated with adding headers during fragmentation, and then the cost associated with defragmenting and reassembling packets, sometimes at multiple points along the transmission path. Because different protocols reserve different numbers of bytes for headers, it's difficult at best to determine an MTU that will always work, especially if you send encrypted data across the Internet, between LANs.

Identifying the Real Problem

You can start solving path MTU problems by issuing a Ping command to your destination host and setting advanced options such as Packet Size and Don't Fragment (DF) in their respective fields.

MORE? You can find a detailed description of this process in the Interface Troubleshooting chapter of *Junos Enterprise Routing*, by Marschke and Reynolds, O'Reilly, 2008.

As shown in Figure 6.6, the J-Web Ping tool is configured to Ping a host by IP address, with the DF option selected, and a packet size of 1500 bytes. Although MTU 1500 is a typical default value, most network administrators modify the MTU for performance reasons.

Ping Host

The ping diagnostic tool sends a series of ICMP "echo request" packets to the specified remote host.

The receipt of such packets will usually result in the remote host replying with an ICMP "echo response." Note that some hosts are configured not to respond to ICMP "echo requests," so a lack of responses does not necessarily represent a connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you may find that you are not able to ping outside your local network.

Entering a host below creates a periodic ping task that will run until cancelled or until it times out as specified.

* Remote Host:

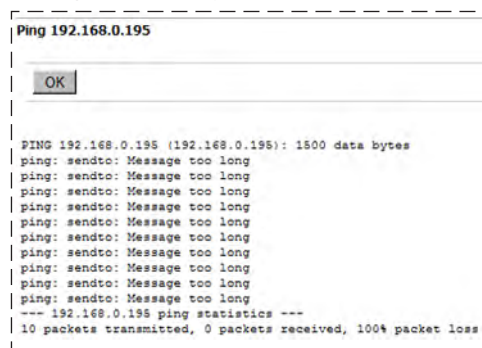
Advanced options

Don't Resolve Addresses <input type="checkbox"/>	Routing Instance: <input type="text" value="default"/>
Interface: <input type="text" value="any"/>	Interval: <input type="text" value="1"/>
Count: <input type="text" value="10"/>	Packet Size: <input type="text" value="1501"/>
Don't Fragment <input checked="" type="checkbox"/>	Source Address: <input type="text"/>
Record Route <input type="checkbox"/>	Time-to-Live: <input type="text" value="32"/>
Type-of-Service: <input type="text" value="0"/>	Bypass Routing <input type="checkbox"/>

Figure 6.6 Setting the Don't Fragment Option

It is also important to remember that the MTU value includes any bytes that are reserved to accommodate the header of whichever protocols you are running. So, even though you may ping the host to see if it will accept a packet of 1500 bytes, the maximum packet size is really slightly smaller than that, depending on which protocols the host is running.

In Figure 6.7 the output shows that the host does not support packets as large as 1500 bytes.



```
Ping 192.168.0.195
OK

PING 192.168.0.195 (192.168.0.195): 1500 data bytes
ping: sendto: Message too long
ping: sendto: Message too long
ping: sendto: Message too long
ping: sendto: Message too long
ping: sendto: Message too long
ping: sendto: Message too long
ping: sendto: Message too long
ping: sendto: Message too long
ping: sendto: Message too long
ping: sendto: Message too long
--- 192.168.0.195 ping statistics ---
10 packets transmitted, 0 packets received, 100% packet loss
```

Figure 6.7 Identifying the Packet Size Error

As you can see, Ping returns an ICMP error that the message is too long. Additionally, the statistics note that 0 packets were received by the host and there was 100% packet loss. Obviously, this isn't an optimal situation.

The host requires an MTU smaller than the MTU of your egress interface, in this case, 1500 bytes. Because you set the DF option, the intermediate host did not attempt to fragment the packet, but simply dropped it and returned an ICMP error.

Discovering this problem by using Ping is much less costly than discovering the problem when your users start to complain that they aren't getting the results they expected. Unfortunately, there is no single solution to the fragmentation problem. The solution depends on a variety of factors including bandwidth and performance requirements.

The simplest, but perhaps most crude, solution is to set the MTU of the intermediate device to be higher, assuming you have control over that device. You can also set the MTU of your egress interface to match the lower value on the host, which will cause your device to send smaller

packets. These smaller packets will be less likely to be fragmented, as shown in Figure 6.8.

```

Ping Host
Ping 172.23.6.117
OK

PING 172.23.6.117 (172.23.6.117): 1372 data bytes
1380 bytes from 172.23.6.117: icmp_seq=0 ttl=122 time=49.148 ms
1380 bytes from 172.23.6.117: icmp_seq=1 ttl=122 time=144.046 ms
1380 bytes from 172.23.6.117: icmp_seq=3 ttl=122 time=106.262 ms
1380 bytes from 172.23.6.117: icmp_seq=4 ttl=122 time=90.106 ms
1380 bytes from 172.23.6.117: icmp_seq=5 ttl=122 time=92.075 ms
1380 bytes from 172.23.6.117: icmp_seq=6 ttl=122 time=91.697 ms
1380 bytes from 172.23.6.117: icmp_seq=7 ttl=122 time=99.549 ms
1380 bytes from 172.23.6.117: icmp_seq=8 ttl=122 time=102.214 ms
1380 bytes from 172.23.6.117: icmp_seq=9 ttl=122 time=94.803 ms
--- 172.23.6.117 ping statistics ---
10 packets transmitted, 9 packets received, 10% packet loss
round-trip min/avg/max/stddev = 49.148/95.988/144.046/22.909 ms
  
```

Figure 6.8 Discovering the Allowable Packet Size of 1372 Bytes

EXPLORE You may want to define security policies for a given interface, restricting traffic to or from a particular host to that interface. By default, Ping requests use the source device's routing table and therefore may use any of the valid routes listed in the table to get to a specified host. If you want to test connectivity to a host over a specified interface, and you want to avoid using the route table, use a combination of the Interface option and the Bypass Routing option. Try the various options using Ping with J-Web.

Practice: Identifying Hosts with Traceroute

Traceroute helps you identify the hosts along the path to your destination. There are several situations in which you might want to use traceroute. For example, if you can't get a response from a host when using the Ping command, you might want to run traceroute to see if the host is down or if you are running into an intermediate system that is offline, which is getting in the way before you can even get to the destination host.

Another common problem is network latency. The traceroute output will provide you with a round-trip response time from each device along the path to your destination. You can use the output response times to determine latency issues with one or more hosts in your path.

MORE? You can find a complete list of traceroute options in the *Junos Security Administration Guide* at <http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-admin-guide/index.htm>

Traceroute output is not difficult to understand. For example, you can identify latency problems by noting which devices take longest to respond.

One thing to note in traceroute output is when you see one or more asterisks (*) in the output. When you see asterisks in an intermediate host response, the asterisks mean that the request was dropped or somehow rejected. There can be a number of reasons for this:

- The device is down.
- The device is configured to ignore ICMP traceroute requests.
- The TTL value you specified is lower than the time it took to get to the device or for the device to respond.

Because traceroute has been abused by hackers over the last few years, many public-facing servers are configured to reject traceroute requests. However, if you are checking a path *within* your own internal network, this should not be an issue.

Nonetheless, traceroute output provides at least two essential indicators for diagnosing your network traffic:

- Round-trip time.
- Request failure, as indicated by asterisks.

You can use both of these indicators to help identify problems in your destination path using J-Web.

Try the traceroute option within the Troubleshooting tab as shown in Figure 6.9. For example, previously, in Figure 6.8's traceroute output, you can see that the response times for each hop are sometimes very slow. This may be a result of heavy traffic to that host, the low priority of the traceroute request, or some other issue. At the bottom of the output, you can see that the traceroute request returns several sets of asterisks. The asterisks indicate that the host is unavailable, the request has timed out, or the host has rejected the request for some reason. In any case, at least you know that you are able to reach the host listed in line 7 before you run into problems.

Traceroute

The traceroute diagnostic tool uses a series of packets crafted to elicit an ICMP "time exceeded" messages from intermediate points in the network between your device and the specified host.

The time-to-live for a packet is decremented each time the packet is routed, so traceroute generally receives at least one "time exceeded" response from each waypoint. Traceroute starts with a packet with a time-to-live value of one, and increments the time to live for subsequent packets, thereby constructing a rudimentary map of the path between hosts.

Entering a host below creates a traceroute task that will run until the traceroute is complete or until it fails due to time out.

Remote Host:

Advanced options

Don't Resolve Addresses: ☐

Interface:

Time-to-Live:

Type-of-Service:

Routing Instance:

Gateway:

Source Address:

Bypass Routing: ☐

Figure 6.9 Setting Traceroute Parameters

Setting the Time-to-Live parameter to a lower number allows you to focus on a smaller number of hops than the default of 32 hops. In this example, Time-to-Live is set to 8 hops. As you can see in Figure 6.10, the rows of asterisks indicate that the trace is unable to reach the hosts following the fifth hop.

Traceroute

Traceroute to 10.254.71.68

OK

```

traceroute to 10.254.71.68 (10.254.71.68), 8 hops max, 40 byte packets
 1  10.157.64.1 (10.157.64.1)  102.239 ms  71.941 ms  4.016 ms
 2  10.149.0.65 (10.149.0.65)  3.624 ms  3.465 ms  3.690 ms
 3  10.149.0.2 (10.149.0.2)  3.814 ms  3.687 ms  3.882 ms
 4  mandalay-ge-link-mrc3-eng-gw1.jnpr.net (172.24.230.181)  4.552 ms  8.702 ms  5.7
 5  172.24.230.90 (172.24.230.90)  6.862 ms  18.973 ms  4.928 ms
 6  * * *
 7  * * *
 8  * * *

```

Figure 6.10 Identifying Route Problems

EXPLORE Try identifying hosts with traceroutes on your testbed or on the SRX device you are using. What do you see? By this time you should be able to explore all the options and features of configuring SRX Series with J-Web.

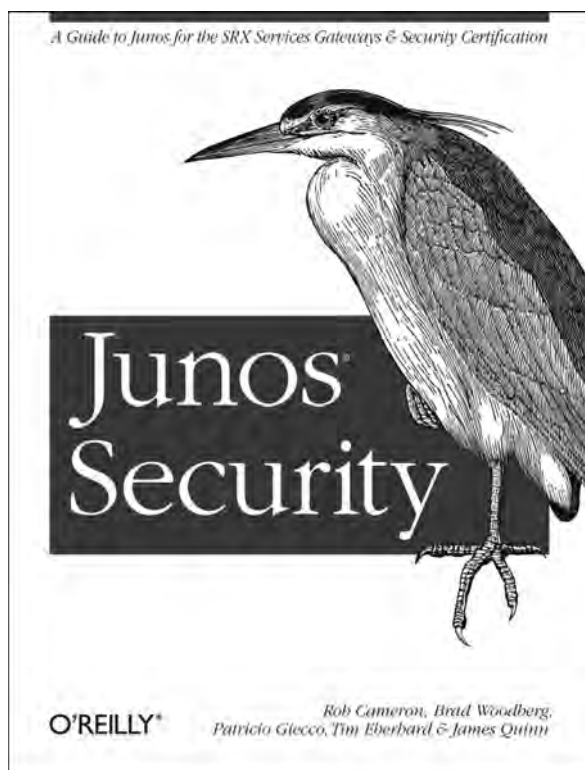
MORE? If you need more information about any of these features, see: *Day One: Deploying SRX Series Services Gateways* at www.juniper.net/dayone; *Junos Security*, by Cameron, et. al., published by O'Reilly Media, at www.juniper.net/books; or, consult the SRX device documentation at www.juniper.net/techpubs.

Summary

As mentioned throughout this book, there are several other troubleshooting tools available for your use on your SRX device. However, Ping and Traceroute should give you a great start on solving connectivity and path problems. For more detailed troubleshooting, review your session logs, as described in Chapter 5 of this book.

The Definitive Guide for the SRX Series Services Gateways

Junos® Security is the complete and authorized introduction to Juniper Network's SRX hardware series running the Junos operating system. This book not only provides a practical hands-on field guide to deploying, configuring, and operating SRX, but also serves as a reference to help you prepare for the JNCIS-ES and JNCIE-ES Certification examinations.



Network administrators and security professionals will learn how to address a whole array of enterprise data network requirements using SRX Junos services gateways – including IP routing, intrusion detection, attack mitigation, unified threat management, and WAN acceleration. Junos Enterprise Security is a clear and detailed roadmap to SRX product lines.

- Get up to speed on Juniper's multi-function SRX platforms and SRX Junos software.
- Learn directly from engineers with extensive experience using SRX.
- Take advantage of the authors' knowledge through case studies and troubleshooting tips.
- Become familiar with SRX security policy, Network Address Translation, and IPSec VPN configuration.
- Learn about routing fundamentals and high availability on SRX platforms.

Available wherever technical books are sold. For more information about this or other titles in the *Juniper Networks Technical Library* go to: www.juniper.net/books.

What to Do Next & Where to Go

www.juniper.net/dayone

This book is available in multiple formats, including ebook formats for your mobile devices. Go here to download or find out what other Day One booklets are currently available.

www.juniper.net/junos

Everything you need for Junos adoption and education.

<http://forums.juniper.net/jnet>

The Juniper-sponsored J-Net Communities forum is dedicated to sharing information, best practices, and questions about Juniper products, technologies, and solutions. Register to participate in this free forum.

www.juniper.net/techpubs

All Juniper-developed product documentation is freely accessible at this site. Find what you need to know about the Junos operating system under each product line.

www.juniper.net/books

Juniper works with multiple book publishers to author and publish technical books on topics essential to network administrators. Check out this ever-expanding list of newly published books including the new SRX-specific *Junos Security*.

www.juniper.net/training/fasttrack

Take courses online, on location, or at one of the partner training centers around the world. The Juniper Network Technical Certification Program (JNTCP) allows you to earn certifications by demonstrating competence in configuration and troubleshooting of Juniper products. If you want the fast track to earning your certifications in enterprise routing, switching, or security use the available online courses, student guides, and lab guides.