**JUNOS® Software**

# System Basics Configuration Guide

*Release 9.4*

**Juniper Networks, Inc.**
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
**www.juniper.net**

Part Number: 530-028714-01, Revision 1

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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

*JUNOS® Software System Basics Configuration Guide*
Release 9.4
Copyright © 2009, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Lisa Kelly, Bruce Gillham, Stephen Meiers, Michael Scruggs, Joanne McClintock, and Mahesh Anantharaman
Editing: Stella Hackell, Nancy Kurahashi, Sonia Saruba, and Joanne McClintock
Illustration: Faith Bradford
Cover Design: Edmonds Design

Revision History
15 January 2009—Revision 1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

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

## END USER LICENSE AGREEMENT

**READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

# Abbreviated Table of Contents

# Table of Contents

## Part 6 Router Chassis

### Chapter 24 Router Chassis Configuration Guidelines 707

## Part 7 Index

# List of Figures

# List of Tables

# About This Guide

This preface provides the following guidelines for using the *JUNOS® Software System Basics Configuration Guide*:



## Objectives

This guide describes Juniper Networks routing platforms, and provides information about how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router.

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M-series, MX-series, T-series, EX-series, or J-series router or switch.

**NOTE:** This guide documents Release 9.4 of the JUNOS internet software. For additional information about JUNOS software—either corrections to or information that might have been omitted from this guide—see the software release notes at http://www.juniper.net.

## Audience

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)

- Intermediate System-to-Intermediate System (IS-IS)
- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

## Supported Platforms

For the features described in this manual, the JUNOS software currently supports the following platforms:

- J-series
- M-series
- MX-series
- T-series
- EX-series

## Using the Indexes

This reference contains two indexes: a standard index with topic entries, and an index of commands.

## Using the Examples in This Manual

If you want to use the examples in this manual, you can use the load merge or the load merge relative command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the load merge command.

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

### *Merging a Full Example*

To merge a full example, follow these steps:

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

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

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

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

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

### *Merging a Snippet*

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

For more information about the load command, see the *JUNOS CLI User Guide*.

## Documentation Conventions

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

**Table 1: Notice Icons**

| Icon | Meaning | Description |
|---|---|---|
|  | Informational note | Indicates important features or instructions. |
|  | Caution | Indicates a situation that might result in loss of data or hardware damage. |
|  | Warning | Alerts you to the risk of personal injury or death. |
|  | Laser warning | Alerts you to the risk of personal injury from a laser. |

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

**Table 2: Text and Syntax Conventions**

| Convention | Description | Examples |
|---|---|---|
| Bold text like this | Represents text that you type. | To enter configuration mode, type the configure command:<br>user@host> **configure** |
| `Fixed-width text like this` | Represents output that appears on the terminal screen. | `user@host> show chassis alarms`<br>`No alarms currently active` |

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

| Convention | Description | Examples |
|---|---|---|
| *Italic text like this* | ■ Introduces important new terms.<br>■ Identifies book names.<br>■ Identifies RFC and Internet draft titles. | ■ A policy *term* is a named structure that defines match conditions and actions.<br>■ *JUNOS System Basics Configuration Guide*<br>■ RFC 1997, *BGP Communities Attribute* |
| *Italic text like this* | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name:<br>[edit]<br>root@# **set system domain-name** *domain-name* |
| Plain text like this | Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components. | ■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.<br>■ The console port is labeled CONSOLE. |
| < > (angle brackets) | Enclose optional keywords or variables. | stub <default-metric *metric*>; |
| \| (pipe symbol) | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | broadcast \| multicast<br>(*string1* \| *string2* \| *string3*) |
| # (pound sign) | Indicates a comment specified on the same line as the configuration statement to which it applies. | rsvp { # Required for dynamic MPLS only |
| [ ] (square brackets) | Enclose a variable for which you can substitute one or more values. | community name members [ *community-ids* ] |
| Indention and braces ( { } ) | Identify a level in the configuration hierarchy. | [edit]<br>routing-options {<br>  static {<br>  route default {<br>  nexthop *address*;<br>  retain;<br>  }<br>  }<br>} |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| **J-Web GUI Conventions** | | |
| **Bold text like this** | Represents J-Web graphical user interface (GUI) items you click or select. | ■ In the Logical Interfaces box, select **All Interfaces**.<br>■ To cancel the configuration, click **Cancel**. |
| > (bold right angle bracket) | Separates levels in a hierarchy of J-Web selections. | In the configuration editor hierarchy, select **Protocols > Ospf**. |

## List of Technical Publications

Table 3 on page xlii lists the software and hardware guides and release notes for Juniper Networks M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 4 on page xlvi lists the books included in the *Network Operations Guide* series. Table 5 on page xlvii lists the manuals and release notes supporting JUNOS software for J-series and SRX-series platforms. All documents are available at http://www.juniper.net/techpubs/.

Table 6 on page xlviii lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at http://www.juniper.net/books.

**Table 3: Technical Documentation for Supported Routing Platforms**

| Book | Description |
|---|---|
| **JUNOS Software for Supported Routing Platforms** | |
| *Access Privilege* | Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements. |
| *Broadband Subscriber Management Solutions* | Describes residential subscriber management and how you can deploy solutions that include multisubscriber IP address assignment, service provisioning, authentication, authorization, accounting, and dynamic request services in your network |
| *Class of Service* | Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm. |
| *CLI User Guide* | Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the *JUNOS System Basics Configuration Guide*. |
| *Feature Guide* | Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software. |
| *High Availability* | Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop active routing (NSR) and graceful Routing Engine switchover (GRES). |
| *MPLS Applications* | Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols. |
| *Multicast Protocols* | Provides an overview of multicast concepts and describes how to configure multicast routing protocols. |

**Table 3: Technical Documentation for Supported Routing Platforms** *(continued)*

| Book | Description |
|---|---|
| *Multiplay Solutions* | Describes how you can deploy IPTV and voice over IP (VoIP) services in your network. |
| *MX-series Layer 2 Configuration Guide* | Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the *JUNOS Routing Protocols Configuration Guide*. |
| *MX-series Layer 2 Solutions Guide* | Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB). |
| *Network Interfaces* | Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform. |
| *Network Management* | Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options. |
| *Policy Framework* | Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options. |
| *Protected System Domain* | Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration. |
| *Routing Protocols* | Provides an overview of routing concepts and describes how to configure routing instances, and unicast routing protocols. |
| *Secure Configuration Guide for Common Criteria and JUNOS-FIPS* | Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform. |
| *Services Interfaces* | Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router. |
| *Software Installation and Upgrade Guide* | Describes the JUNOS software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the *JUNOS System Basics Configuration Guide*. |

**Table 3: Technical Documentation for Supported Routing Platforms** *(continued)*

| Book | Description |
|---|---|
| *Subscriber Access* | Provides an overview of the subscriber access features of the JUNOS software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods. |
| *System Basics* | Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network. |
| *VPNs* | Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples. |
| **JUNOS References** | |
| *Hierarchy and RFC Reference* | Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the *JUNOS System Basics Configuration Guide*. |
| *Interfaces Command Reference* | Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces. |
| *Routing Protocols and Policies Command Reference* | Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters. |
| *System Basics and Services Command Reference* | Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPsec), stateful firewalls, flow collection, and flow monitoring. |
| *System Log Messages Reference* | Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message. |
| **J-Web User Guide** | |
| *J-Web Interface User Guide* | Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms. |
| **JUNOS API and Scripting Documentation** | |
| *JUNOScript API Guide* | Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms. |
| *JUNOS XML API Configuration Reference* | Provides reference pages for the configuration tag elements in the JUNOS XML API. |

**Table 3: Technical Documentation for Supported Routing Platforms** *(continued)*

| Book | Description |
|---|---|
| *JUNOS XML API Operational Reference* | Provides reference pages for the operational tag elements in the JUNOS XML API. |
| *NETCONF API Guide* | Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms. |
| *JUNOS Configuration and Diagnostic Automation Guide* | Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies. |
| **Hardware Documentation** | |
| *Hardware Guide* | Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide. |
| *PIC Guide* | Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide. |
| *DPC Guide* | Describes the Dense Port Concentrators (DPCs) for all MX-series routers. |
| **JUNOScope Documentation** | |
| *JUNOScope Software User Guide* | Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations. |
| **Advanced Insight Solutions (AIS) Documentation** | |
| *Advanced Insight Solutions Guide* | Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices. |
| **Release Notes** | |
| *JUNOS Release Notes* | Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures. |
| *Hardware Release Notes* | Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes. |
| *JUNOScope Release Notes* | Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures. |

**Table 3: Technical Documentation for Supported Routing Platforms** *(continued)*

| Book | Description |
|---|---|
| *AIS Release Notes* | Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures. |
| *AIS AI-Scripts Release Notes* | Summarize AI-Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back. |

**Table 4: JUNOS Software Network Operations Guides**

| Book | Description |
|---|---|
| *Baseline* | Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages. |
| *Interfaces* | Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms. |
| *MPLS* | Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network. |
| *MPLS Log Reference* | Describes MPLS status and error messages that appear in the output of the show mpls lsp extensive command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network. |
| *MPLS Fast Reroute* | Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing. |
| *Hardware* | Describes tasks for monitoring M-series and T-series routing platforms. |

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

**Table 5: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation**

| Book | Description |
|---|---|
| **J-series and SRX-series Platforms** | |
| *JUNOS Software Interfaces and Routing Configuration Guide* | Explains how to configure SRX-series and J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification. |
| *JUNOS Software Security Configuration Guide* | Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP). |
| *JUNOS Software Administration Guide* | Shows how to monitor SRX-series and J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems. |
| *JUNOS Software CLI Reference* | Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices. |
| *JUNOS Release Notes* | Summarize new features and known problems for a particular release of JUNOS software, including JUNOS software for J-series and SRX-series devices.The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software. |
| **J-series Only** | |
| *JUNOS Software Design and Implementation Guide* | Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS software. |
| *J-series Services Routers Quick Start* | Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity. |
| *J-series Services Routers Hardware Guide* | Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications. |
| *JUNOS Software Migration Guide* | Provides instructions for migrating an SSG device running ScreenOS software to JUNOS software or upgrading a J-series device to a later version of the JUNOS software. |
| *WXC Integrated Services Module Installation and Configuration Guide* | Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration. |

**Table 6: Additional Books Available Through http://www.juniper.net/books**

| Book | Description |
|---|---|
| *Interdomain Multicast Routing* | Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms. |
| *JUNOS Cookbook* | Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs. |
| *MPLS-Enabled Applications* | Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks. |
| *OSPF and IS-IS: Choosing an IGP for Large-Scale Networks* | Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks. |
| *Routing Policy and Protocols for Multivendor IP Networks* | Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers. |
| *The Complete IS-IS Protocol* | Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach. |

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for *Network Operations Guides [NOGs])*

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

### Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

### Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html.

# Part 1
# Overview

Chapter 1

# Introduction to JUNOS Software

Juniper Networks provides high-performance network routing platforms that create a responsive and trusted environment for accelerating the deployment of services and applications over a single network. The JUNOS software is the foundation of these high-performance networks. Unlike other complex, monolithic software architectures, the JUNOS software incorporates key design and developmental differences to deliver increased network availability, operational efficiency, and flexibility. The key advantages of this approach are:

- One operating system
- One software release
- One modular software architecture

### One Operating System

Unlike other network operating systems that share a common name but splinter into many different programs, the JUNOS software is a single, cohesive operating system that is shared across all routers and product lines. This approach allows Juniper Network engineers to develop software features once and share that feature across all of our product lines simultaneously. Because features are common to a single source, generally these features are implemented the same way for all the product lines, thus reducing the training required to learn different tools and methods for each product. Because all Juniper Networks products use the same code base, interoperability between products is not an issue.

### One Software Release

Each new version of the JUNOS software is released concurrently for all product lines. Each new version of the software must include all working features released in previous releases of the software and must achieve zero critical regression errors. This discipline ensures reliable operations for the entire release.

### One Modular Software Architecture

Although individual modules of the JUNOS software communicate through well-defined interfaces, each module runs in its own protected memory space, preventing one module from disrupting another. It also allows the independent restart of each module as necessary. This is in contrast to monolithic operating systems for which a malfunction in one module can ripple to others and cause a full system crash or restart. This modular architecture then provides for a high level of performance, high availability, security, and device scalability not found in other operating systems.

The rest of this chapter discusses the following:



## Product Architecture

The JUNOS software provides IP routing protocol software as well as software for interface, network, and chassis management. The JUNOS software runs on all Juniper Networks J-series, M-series, MX-series, and T-series routing platforms.

- J-series Services Routers (J2300, J4300, and J6300) are deployed at the remote edge of distributed networks.
- Most M-series routers are deployed in small and medium cores in peering, route reflector, data center applications; or at the IP or Multiprotocol Label Switching (MPLS) edge to support high-performance Layer 2 and Layer 3 services. All M-series routers have redundant power and cooling and the M10i, M20, M40e, M120, M160, and M320 routers have fully redundant hardware, including Routing Engines, switch interface components, and packet forwarding components. The M120 router also supports Forwarding Engine Board (FEB) failover. In the event of a FEB failure, a backup FEB can quickly take over packet forwarding.
- The MX-series Ethernet Services Routers are Ethernet-optimized edge routers that provide both switching and carrier-class Ethernet routing. The MX-series routers support two types of Dense Port Concentrators (DPCs) with built-in Ethernet ports: Gigabit Ethernet 40-port and 10-Gigabit Ethernet 4-port.
- T-series routing platforms (T320 router, T640 router, and TX Matrix platform) are deployed at the core of provider networks. These routing platforms have fully redundant hardware, including power and cooling, Routing Engines, and Switch Interface Boards.

  A *routing matrix* is a multichassis architecture composed of one TX Matrix platform and from one to four T640 routing nodes. From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix platform controls all the T640 routing nodes on the routing matrix.

For more information about the architecture in your routing platform, see the hardware guide for your routing platform.

This section provides an overview of the router hardware for routing platforms and discusses the relationships between the hardware and software:



### *Hardware Overview*

The JUNOS software runs on four types of Juniper Networks routing platforms: J-series, M-series, MX-series, and T-series. The routing platforms consist of the major hardware

components as shown in Table 7 on page 5. One or more of the major hardware components shown is used in each system.

**Table 7: Major Router Hardware Components**

| | M-series | MX-series | T-series | J-series |
|---|---|---|---|---|
| **Routing Engines (RE)** | X | X | X | X |
| **Control Board** | X | | X | |
| **Switch Interface Board (SIB)** | X | | X | |
| **Forwarding Engine Board (FEB)** | X | | | |
| **Power Supply** | X | X | X | X |
| **Cooling System** | X | X | X | X |
| **Dense Port Concentrators (DPC)** | | X | | |
| **Switch Control Board (SCB)** | | X | | |
| **Flexible PIC Concentrators (FPC)** | X | | X | |
| **Physical Interface Module (PIM)** | | | | X |
| **Physical Interface Card (PIC)** | X | | X | |

Flexible PIC Concentrators (FPCs) are each populated by PICs for various interface types. On some routing platforms, the PICs are installed directly in the chassis.

For information about specific components in your routing platform, see the hardware guide for your routing platform.

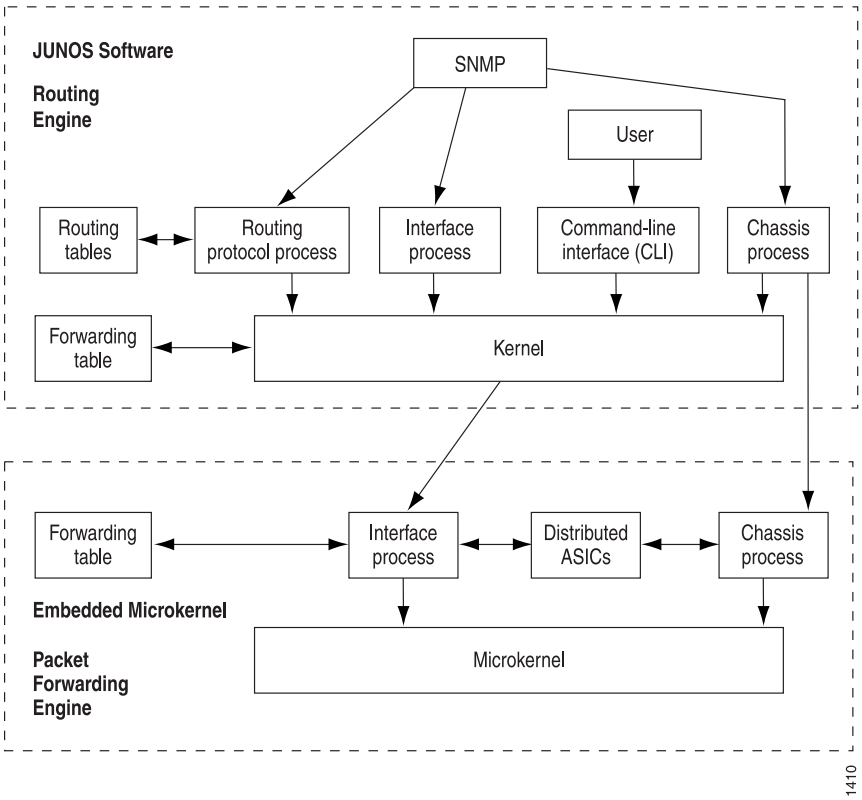
## *Routing Process Architecture*

The routing process is handled by the following two components (see Figure 1 on page 6):

- The Routing Engine
- The Packet Forwarding Engine

Because this architecture separates control operations such as routing updates and system management from packet forwarding, the router can deliver superior performance and highly reliable Internet operation.

**Figure 1: Product Architecture**




## Packet Forwarding Engine

The Packet Forwarding Engine uses application-specific integrated circuits (ASICs) to perform Layer 2 and Layer 3 packet switching, route lookups, and packet forwarding. The Packet Forwarding Engine forwards packets between input and output interfaces. The M-series routers (except the M7i, M40, and M320 routers) have redundant Packet Forwarding Engines. The J-series Services Routers have a software-based Packet Forwarding Engine. For more information about the Packet Forwarding Engine, see the hardware guide for your routing platform.

## Routing Engine

The Routing Engine controls the routing updates and system management. The Routing Engine consists of routing protocol software processes running inside a protected memory environment on a general-purpose computer platform. The Routing Engine handles all the routing protocol processes and other software processes that control the routing platform's interfaces, some of the chassis components, system management, and user access to the routing platform. These routing platform and software processes run on top of a kernel that interacts with the Packet Forwarding Engine. All M-series (except the M7i and M40) routing platforms and T-series routing platforms have redundant Routing Engines. For more information about routers with redundant Routing Engines, see the hardware guide for your routing platform.

The Routing Engine has these features:

- Routing protocol packets processing—All routing protocol packets from the network are directed to the Routing Engine, and therefore do not delay the Packet Forwarding Engine unnecessarily.
- Software modularity—Software functions have been divided into separate processes, so a failure of one process has little or no effect on other software processes.
- In-depth IP functionality—Each routing protocol is implemented with a complete set of IP features and provides full flexibility for advertising, filtering, and modifying routes. Routing policies are set according to route parameters, such as prefix, prefix lengths, and Border Gateway Protocol (BGP) attributes.
- Scalability—The JUNOS routing tables are designed to hold all the routes used in current and near-future networks. Additionally, the JUNOS software can efficiently support large numbers of interfaces and virtual circuits.
- Management interfaces—System management is possible with a command-line interface (CLI), a craft interface, and Simple Network Management Protocol (SNMP).
- Storage and change management—Configuration files, system images, and microcode can be held and maintained in one primary and two secondary storage systems, permitting local or remote upgrades.
- Monitoring efficiency and flexibility—Alarms can be generated and packets can be counted without adversely affecting packet forwarding performance.

The Routing Engine constructs and maintains one or more routing tables. From the routing tables, the Routing Engine derives a table of active routes, called the *forwarding table*, which is then copied into the Packet Forwarding Engine. The forwarding table in the Packet Forwarding Engine can be updated without interrupting the routing platform's forwarding.

In a JUNOS-FIPS environment, hardware configurations with two Routing Engines must use IPSec and a private routing instance for all communications between the Routing Engines. IPSec communication between the Routing Engines and Adaptive Services (AS) II FIPS PICs is also required.

## *Configuration Architecture*

The router configuration is saved using a commit model: a candidate configuration is modified as desired and then committed to the system. Once committed, the router checks the configuration for syntax errors and if no errors are found, the configuration is saved as juniper.conf.gz and activated. The former active configuration file is saved as the first rollback configuration file (juniper.conf.1.gz) and all other rollback configuration files are incremented by 1. For example, juniper.conf.1.gz is incremented to juniper.conf.2.gz, making it the second rollback configuration file. The router can have a maximum of 49 rollback configurations (1–49) saved on the system.

On the router, the active configuration file and the first three rollback files (juniper.conf.gz.1, juniper.conf.gz.2, juniper.conf.gz.3 ) are located in the /config directory. If the recommended rescue file rescue.conf.gz is saved on the system, this

file should also be saved in the /config directory. The factory default files are located in the /etc/config directory.

There are two mechanisms used to propagate the configurations between Routing Engines within a routing platform:

- Synchronization—Propagates a configuration from one Routing Engine to a second Routing Engine within the same router chassis.

  To synchronize a router's configurations, use the commit synchronize CLI command. If one of the Routing Engines is locked, the synchronization fails. If synchronization fails because of a locked configuration file, you can use the commit synchronize force command. This command overrides the lock and synchronizes the configuration files.

- Distribution—Propagates a configuration across the routing plane on a multichassis routing platform. Distribution occurs automatically. There is no user command available to control the distribution process. If a configuration is locked during a distribution of a configuration, the locked configuration does not receive the distributed configuration file, so the synchronization fails. You need to clear the lock before the configuration and resynchronize the routing planes.

**NOTE:** When you use the commit synchronize force CLI command on a multichassis platform, the forced synchronization of the configuration files does not affect the distribution of the configuration file across the routing plane. If a configuration file is locked on a router remote from the router where the command was issued, the synchronization fails on the remote router. You need to clear the lock and reissue the synchronization command.

## JUNOS Software Components

The JUNOS system software runs on the Routing Engine. The JUNOS system software consists of software processes that support Internet routing protocols, control router interfaces and the router chassis, and allow router system management. The JUNOS software processes run on top of a kernel, which enables communication between processes and provides a direct link to the Packet Forwarding Engine software. The JUNOS software can be used to configure routing protocols and router interface properties, as well as to monitor and troubleshoot protocol and network connectivity problems.

**NOTE:** For more information about monitoring the router and troubleshooting problems, see the *JUNOS System Basics and Services Command Reference*, the *JUNOS Interfaces Command Reference*, and the *JUNOS Routing Protocols and Policies Command Reference*.

## Routing Engine Software

The Routing Engine software consists of several software processes that control router functionality and a kernel that provides the communication among all the processes. This section describes the Routing Engine components:



For information about Routing Engine software components and Routing Engine functions in a routing matrix, see the *TX Matrix Platform Hardware Guide*.

### *Routing Engine Kernel*

The Routing Engine kernel provides the underlying infrastructure for all JUNOS software processes. In addition, it provides the link between the routing tables and the Routing Engine's forwarding table. It is also responsible for all communication with the Packet Forwarding Engine, which includes keeping the Packet Forwarding Engine's copy of the forwarding table synchronized with the master copy in the Routing Engine.

### *Initialization Process*

Within the JUNOS software, an initialization process (init) starts and monitors all the other software processes when the router boots.

If a software process terminates or fails to start when called, the init process attempts to restart it a limited number of times and logs any failure information for further investigation.

### *Management Process*

The management process (mgd) manages the configuration of the router and all user commands. The management process is responsible for notifying other daemons when a new configuration is committed. A dedicated management process handles JUNOScript XML requests from its client, which may be the command-line interface (CLI) or any JUNOScript client.

## Process Limits

There are limits to the total number of JUNOS software processes that can run simultaneously on a system. There are also limits set for the maximum number iterations of any single process. The limit for iterations of any single process can only be reached if the limit of overall system processes is not exceeded.

Access methods such as telnet and SSH spawn multiple system processes for each session created. For this reason, it might not be possible to simultaneously support the maximum number of access sessions for multiple services.

## Routing Protocol Process

Within the JUNOS software, the routing protocol process (rpd) controls the routing protocols that run on the router. This process starts all configured routing protocols and handles all routing messages. It maintains one or more routing tables, which consolidate the routing information learned from all routing protocols. From this routing information, the routing protocol process determines the active routes to network destinations and installs these routes into the Routing Engine's forwarding table. Finally, it implements routing policy, which allows you to control the routing information that is transferred between the routing protocols and the routing table. Using routing policy, you can filter and limit the transfer of information as well as set properties associated with specific routes.

This section discusses the following topics:



### IPv4 Routing Protocols

JUNOS system software implements full IP routing functionality, providing support for IP version 4 (IPv4). The routing protocols are fully interoperable with existing IP routing protocols, and they have been developed to provide the scale and control necessary for the Internet core.

JUNOS software provides the following routing and Multiprotocol Label Switching (MPLS) applications protocols:

- Unicast routing protocols:
  - BGP—Border Gateway Protocol, version 4, is an exterior gateway protocol (EGP) that guarantees loop-free exchange of routing information between routing domains (also called autonomous systems). BGP, in conjunction with JUNOS routing policy, provides a system of administrative checks and balances that can be used to implement peering and transit agreements.
  - ICMP—Internet Control Message Protocol router discovery allows hosts to discover the addresses of operational routers on the subnet.

- IS-IS—Intermediate System-to-Intermediate System is a link-state interior gateway protocol (IGP) for IP networks that uses the shortest-path-first (SPF) algorithm, which also is referred to as the Dijkstra algorithm, to determine routes. The JUNOS IS-IS software is a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
- OSPF—Open Shortest Path First, version 2, is an IGP that was developed for IP networks by the Internet Engineering Task Force (IETF). OSPF is a link-state protocol that makes routing decisions based on the SPF algorithm. The JUNOS OSPF software is a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
- RIP—Routing Information Protocol, version 2, is an IGP for IP networks based on the Bellman-Ford algorithm. RIP is a distance-vector protocol. RIP dynamically routes packets between a subscriber and a service provider without the subscriber having to configure BGP or participate in the service provider's IGP discovery process.

- Multicast routing protocols:
  - DVMRP—Distance Vector Multicast Routing Protocol is a dense-mode (flood-and-prune) multicast routing protocol.
  - IGMP—Internet Group Management Protocol, versions 1 and 2, is used to manage membership in multicast groups.
  - MSDP—Multicast Source Discovery Protocol allows multiple Protocol Independent Multicast (PIM) sparse mode domains to be joined. A rendezvous point (RP) in a PIM sparse mode domain has a peer relationship with an RP in another domain, enabling it to discover multicast sources from other domains.
  - PIM sparse mode and dense mode—Protocol-Independent Multicast is a multicast routing protocol. PIM sparse mode routes to multicast groups that might span wide-area and interdomain internets. PIM dense mode is a flood-and-prune protocol.
  - SAP/SDP—Session Announcement Protocol and Session Description Protocol handle conference session announcements.

- MPLS applications protocols:
  - LDP—The Label Distribution Protocol provides a mechanism for distributing labels in nontraffic-engineered applications. LDP allows routers to establish label-switched paths (LSPs) through a network by mapping network-layer routing information directly to data-link layer switched paths. LSPs created by LDP can also traverse LSPs created by the Resource Reservation Protocol (RSVP).
  - MPLS—Multiprotocol Label Switching, formerly known as tag switching, allows you to manually or dynamically configure LSPs through a network. It lets you direct traffic through particular paths rather than rely on the IGP's least-cost algorithm to choose a path.
  - RSVP—The Resource Reservation Protocol, version 1, provides a mechanism for engineering network traffic patterns that is independent of the shortest path decided upon by a routing protocol. RSVP itself is not a routing protocol;

it operates with current and future unicast and multicast routing protocols. The primary purpose of the JUNOS RSVP software is to support dynamic signaling for MPLS LSPs.

### IPv6 Routing Protocols

The JUNOS software implements IP routing functionality, providing support for IP version 6 (IPv6). The routing protocols have been developed to provide the scale and control necessary for the Internet core.

The software supports the following unicast routing protocols:

- BGP—Border Gateway Protocol version 4, is an EGP that guarantees loop-free exchange of routing information between routing domains (also called autonomous systems). BGP, in conjunction with JUNOS routing policies, provides a system of administrative checks and balances that can be used to implement peering and transit agreements.
- ICMP—Internet Control Message Protocol router discovery allows hosts to discover the addresses of operational routers on the subnet.
- IS-IS—Intermediate System-to-Intermediate System is a link-state IGP for IP networks that uses the SPF algorithm, which also is referred to as the Dijkstra algorithm, to determine routes. The JUNOS software supports a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
- OSPF version 3 (OSPFv3) supports IPv6. The fundamental mechanisms of OSPF such as flooding, designated router (DR) election, area-based topologies, and the SPF calculations remain unchanged. Some differences exist either because of changes in protocol semantics between IPv4 and IPv6, or because of the need to handle the increased address size of IPv6.
- RIP—Routing Information Protocol version 2 is an IGP for IP networks based on the Bellman-Ford algorithm. RIP is a distance-vector protocol. RIP dynamically routes packets between a subscriber and a service provider without the subscriber having to configure BGP or to participate in the service provider's IGP discovery process.

### Routing and Forwarding Tables

A major function of the JUNOS routing protocol process is to maintain the Routing Engine's routing tables and from these tables determine the active routes to network destinations. The routing protocol process then installs these routes into the Routing Engine's forwarding table. The JUNOS kernel then copies this forwarding table to the Packet Forwarding Engine.

The routing protocol process maintains multiple routing tables. By default, it maintains the following three routing tables. You can configure additional routing tables to suit your requirements.

- Unicast routing table—Stores routing information for all unicast routing protocols running on the router. BGP, IS-IS, OSPF, and RIP all store their routing information in this routing table. You can configure additional routes, such as static routes,

to be included in this routing table. BGP, IS-IS, OSPF, and RIP use the routes in this routing table when advertising routing information to their neighbors.

- Multicast routing table (cache)—Stores routing information for all the running multicast protocols. DVMRP and PIM both store their routing information in this routing table, and you can configure additional routes to be included in this routing table.
- MPLS routing table—Stores MPLS path and label information.

With each routing table, the routing protocol process uses the collected routing information to determine active routes to network destinations.

For unicast routes, the routing protocol process determines active routes by choosing the most preferred route, which is the route with the lowest preference value. By default, the route's preference value is simply a function of how the routing protocol process learned about the route. You can modify the default preference value using routing policy and with software configuration parameters.

For multicast traffic, the routing protocol process determines active routes based on traffic flow and other parameters specified by the multicast routing protocol algorithms. The routing protocol process then installs one or more active routes to each network destination into the Routing Engine's forwarding table.

### Routing Policy

By default, all routing protocols place their routes into the routing table. When advertising routes, the routing protocols by default advertise only a limited set of routes from the routing table. Specifically, each routing protocol exports only the active routes that were learned by that protocol. In addition, the interior gateway protocols (IS-IS, OSPF, and RIP) export the direct (interface) routes for the interfaces on which they are explicitly configured.

You can control the routes that a protocol places into each table and the routes from that table that the protocol advertises. You do this by defining one or more routing policies and then applying them to the specific routing protocol.

Routing policies applied when the routing protocol places routes into the routing table are referred to as *import policies* because the routes are being imported into the routing table. Policies applied when the routing protocol is advertising routes that are in the routing table are referred to as *export policies* because the routes are being exported from the routing table. In other words, the terms *import* and *export* are used with respect to the routing table.

A routing policy allows you to control (filter) which routes a routing protocol imports into the routing table and which routes a routing protocol exports from the routing table. A routing policy also allows you to set the information associated with a route as it is being imported into or exported from the routing table. Filtering imported routes allows you to control the routes used to determine active routes. Filtering routes being exported from the routing table allows you to control the routes that a protocol advertises to its neighbors.

You implement routing policy by defining policies. A policy specifies the conditions to use to match a route and the action to perform on the route when a match occurs.

For example, when a routing table imports routing information from a routing protocol, a routing policy might modify the route's preference, mark the route with a color to identify it and allow it to be manipulated later, or prevent the route from even being installed in a routing table. When a routing table exports routes into a routing protocol, a policy might assign metric values, modify the BGP community information, tag the route with additional information, or prevent the route from being exported altogether. You also can define policies for redistributing the routes learned from one protocol into another protocol.

### *VPNs*

The JUNOS software supports several types of virtual private networks (VPNs):

- Layer 2 VPNs—A Layer 2 VPN links a set of sites that share routing information, and whose connectivity is controlled by a collection of policies. A Layer 2 VPN is not aware of routes within a customer's network. It simply provides private links between a customer's sites over the service provider's existing public Internet backbone.
- Layer 3 VPNs—A Layer 3 VPN is the same thing as a Layer 2 VPN, but it is aware of routes within a customer's network, requiring more configuration on the part of the service provider than a Layer 2 VPN. The sites that make up a Layer 3 VPN are connected over a service provider's existing public Internet backbone.
- Interprovider VPNs—An interprovider VPN supplies connectivity between two VPNs in separate autonomous systems (ASs). This functionality can be used by a VPN customer with connections to several Internet service providers (ISPs), or different connections to the same ISP in various geographic regions.
- Carrier-of-carrier VPNs—Carrier-of-carrier VPNs allow a VPN service provider to supply VPN service to a customer who is also a service provider. The latter service provider supplies Internet or VPN service to an end customer.

### *Interface Process*

The JUNOS interface process allows you to configure and control the physical interface devices and logical interfaces present in a router. You can configure interface properties such as the interface location (which slot the Flexible PIC Concentrator [FPC] is installed in and which location on the FPC the Physical Interface Card [PIC] is installed in), the interface encapsulation, and interface-specific properties. You can configure the interfaces currently present in the router, as well as interfaces that are not present but that you might add later.

The JUNOS interface process communicates through the JUNOS kernel with the interface process in the Packet Forwarding Engine, enabling the JUNOS software to track the status and condition of the router's interfaces.

### *Chassis Process*

The JUNOS chassis process allows you to configure and control the properties of the router, including conditions that trigger alarms. The chassis process (chassisd) on the Routing Engine communicates directly with its peer processes running on the Packet Forwarding Engine.

### SNMP and MIB II Processes

The JUNOS software supports the Simple Network Management Protocol (SNMP), which helps administrators monitor the state of a router. The software supports SNMP version 1 (SNMPv1), version 2 (SNMPv2, also known as version 2c, or v2c), and version 3 (SNMPv3). The JUNOS implementation of SNMP does not include any of the security features that were originally included in the IETF SNMP drafts but were later dropped. The SNMP software is controlled by the JUNOS SNMP and Management Information Base II (MIB II) processes, which consist of an SNMP master agent and various subagents. For information about SNMP, see the *JUNOS Network Management Configuration Guide*.

Chapter 2

# JUNOS Configuration Basics

Your routing platform comes with JUNOS software installed on it. When you power on the router, all software starts automatically. You simply need to configure the software so that the router will be ready to participate in the network.

To configure the JUNOS software, you must specify a hierarchy of configuration statements that define the preferred software properties. You can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as some system hardware properties. After you have created a candidate configuration, you commit the configuration to be evaluated and activated by the JUNOS software.

This chapter discusses the following topics:



## Configuring the Software from External Devices

You can configure the router from a system console connected to the routing platform's console port or by using Telnet to access the router remotely. The router provides three ports on the craft interface for connecting external management devices to the Routing Engine and the JUNOS software:

- Console port—Connects a system console using an RS-232 serial cable.
- Auxiliary port—Connects a laptop or modem using an RS-232 serial cable.
- Ethernet management port—Connects the Routing Engine to a management LAN (or any other device that plugs into an Ethernet connection) for remote management through a PC or other client device. The Ethernet port is 10/100 megabits per second (Mbps) autosensing and requires an RJ-45 connector.

## Methods for Configuring the JUNOS Software

You can use any of the methods shown in Table 8 on page 18 to configure JUNOS system software:

**Table 8: Methods for Configuring JUNOS Software**

| Method | Description |
|---|---|
| Command-line interface (CLI) | Create the configuration for the router using the CLI. You can enter commands from a single command line, and scroll through recently executed commands. |
| ASCII file | Load an ASCII file containing a router configuration that you created earlier, either on this system or on another system. You can then activate and run the configuration file, or you can edit it using the CLI and then activate it. |
| J-Web graphical user interface (GUI) | Use the J-Web graphical user interface (GUI) to configure the router. J-Web enables you to monitor, configure, troubleshoot, and manage the router on a client by means of a Web browser. The J-Web GUI is preinstalled on J-series Services Routers and is an optional software package that can be installed on M-series and T-series routers. |
| JUNOScript application programming interface (API) | Use JUNOScript Perl client modules to develop custom applications for configuring information on routing platforms that run JUNOS software. Client applications use the JUNOScript API to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. The JUNOScript API is customized for JUNOS software and operations in the API are equivalent to JUNOS CLI. |
| NETCONF application programming interface (API) | Use NETCONF Perl client modules to develop custom applications for configuring information on routing platforms that run JUNOS software. Client applications use the NETCONF API to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. The NETCONF API includes features that accommodate the configuration data models of multiple vendors. |
| Configuration commit scripts | Create scripts that run at commit time to enforce custom configuration rules. Commit scripts are written in Extensible Stylesheet Language Transformations (XSLT). |

This section contains complete descriptions of the following methods you can use to configure JUNOS system software:



## *JUNOS Command-Line Interface (CLI)*

The JUNOS CLI is a straightforward command interface. You use Emacs-style keyboard sequences to move around on a command line and scroll through a buffer that

contains recently executed commands. You type commands on a single line, and the commands are executed when you press the Enter key. The CLI also provides command help and command completion. For more information about the CLI, see the *JUNOS CLI User Guide* and *JUNOS System Basics and Services Command Reference*.

### ASCII File

You can load an ASCII file containing a router configuration that you created earlier, either on this system or another system. You can then activate and run the configuration file as is, or you can edit it using the CLI and then activate it.

### J-Web Package

As an alternative to entering CLI commands, the JUNOS software supports a J-Web graphical user interface (GUI). The J-Web user interface enables you to monitor, configure, troubleshoot, and manage the router on a client by means of a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.

The J-Web user interface is preinstalled on J-series Services Routers. It is provided as an optional, licensed software package (jweb package) on M-series and T-series routing platforms. The jweb package is not included in jinstall and jbundle software bundles. It must be installed separately. To install the package on M-series and T-series routing platforms, follow the procedure described in the *JUNOS Software Installation and Upgrade Guide*.

J-Web supports weak (56-bit) encryption by default. This enables international customers to install J-Web and use HTTPS connections for J-Web access. Domestic customers can also install the jcrypto strong encryption package. This package automatically overrides the weak encryption. For more information about the J-Web GUI, see the *J-Web Interface User Guide*.

**NOTE:** Because the J-Web package is bundled separately from other packages, it is possible to have a version mismatch between J-Web and other JUNOS software packages you have installed.

To check for a version mismatch, use the show system alarms CLI command. If the version number does not match exactly, a system alarm appears. For example, if you install the 7.4R1.2 jroute package and the 7.4R1.1 jweb package, an alarm is activated. For more information on the show system alarms command, see the *JUNOS System Basics and Services Command Reference*.

### JUNOScript API Software

The JUNOScript API is an Extensible Markup Language (XML) application that client applications use to request and change configuration information on Juniper Networks J-series, M-series, MX-series, and T-series routing platforms. This API is customized for JUNOS software, and operations in the API are equivalent to JUNOS CLI configuration mode commands. The JUNOScript API includes a set of Perl modules

that enable client applications to communicate with a JUNOScript server on the router. The Perl modules are used to develop custom applications for configuring and monitoring JUNOS software.

For a complete description of how to use JUNOS XML and JUNOScript API software, see the *JUNOScript API Guide*.

### *NETCONF API Software*

The NETCONF API is an Extensible Markup Language (XML) application that client applications can use to request and change configuration information on Juniper Networks J-series, M-series, MX-series, and T-series routing platforms. This API is customized for JUNOS software, and includes features that accommodate the configuration data models of multiple vendors. The NETCONF API includes a set of Perl modules that enable client applications to communicate with a NETCONF server on the router. The Perl modules are used to develop custom applications for configuring and monitoring JUNOS software.

For a complete description of how to use JUNOS XML and NETCONF API software, see the *NETCONF API Guide*.

### *Configuration Commit Scripts*

You can create and use scripts that run at commit time to enforce custom configuration rules. If a configuration breaks the custom rules, the script can generate actions that the JUNOS software performs. These actions include:

- Generating custom error messages
- Generating custom warning messages
- Generating custom system log messages
- Making changes to the configuration

Configuration commit scripts also enable you to create macros, which expand simplified custom aliases for frequently used configuration statements into standard JUNOS configuration statements. Commit scripts are written in Extensible Stylesheet Language Transformations (XSLT). For more information, see the *JUNOS Configuration and Diagnostic Automation Guide*.

## Configuring a Router for the First Time

On most JUNOS routing platforms, the JUNOS software is installed on the CompactFlash card and on the hard disk. When you first turn on a routing platform, it runs the version of the JUNOS software installed on the CompactFlash card. The copy of JUNOS software on the hard disk is a backup. Another backup copy of the JUNOS software is available on removable media, such as a PC Card or a CompactFlash card. Be sure to put the backup JUNOS software (on removable media) in a safe place.

When you turn on a routing platform the first time, the JUNOS software automatically boots and starts. You must enter basic configuration information so that the routing platform is on the network and you can log in to it over the network.

This section provides the procedures for configuring the JUNOS software on a routing platform with either single or dual Routing Engines:



To configure the routing platform initially, you must connect a terminal or laptop computer to the routing platform through the console port—a serial port on the front of the routing platform. Only console access to the routing platform is enabled by default. Remote management access to the routing platform and all management access protocols, including Telnet, FTP, and SSH, are disabled by default.

When you first connect to the routing platform console, you must log in as the user root. At first, the root account requires no password. You see that you are the user root, because the routing platform command prompt shows the username root@#.

You must start the JUNOS software command-line interface (CLI) using the command cli. The command prompt root@> indicates that you are the user root and that you are in the JUNOS software operational mode. Enter the JUNOS software configuration mode by typing the command configure. The command prompt root@# indicates that you are in the JUNOS software configuration mode.

When you first configure a routing platform, you must configure the following basic properties:

- Routing platform hostname
- Domain name
- IP address of the routing platform Ethernet management interface—fxp0
- IP address of a backup router
- IP address of one or more DNS name servers on your network
- Password for the root account

## *Configuring the JUNOS Software the First Time on a Router with a Single Routing Engine*

To configure the software for the first time, follow these steps:

1. Connect a terminal or laptop computer to the routing platform through the console port—a serial port on the front of the routing platform. Only console access to the routing platform is enabled by default.
2. Power on the routing platform and wait for it to boot.

   The JUNOS software boots automatically. The boot process is complete when you see the login: prompt on the console.
3. Log in as the user root.

   Initially, the root user account requires no password. You can see that you are the root user, because the prompt on the routing platform shows the username root@#.
4. Start the JUNOS software command-line interface (CLI):

   ```
   root@# cli
   root@>
   ```

5. Enter JUNOS software configuration mode:

   ```
   cli> configure
   [edit]
   root@#
   ```

6. Configure the name of the routing platform (the routing platform hostname). We do not recommend spaces in the routing platform name. However, if the name does include spaces, enclose the entire name in quotation marks (" ").

   ```
   [edit]
   root@# set system host-name hostname
   ```

7. Configure the routing platform's domain name:

   ```
   [edit]
   root@# set system domain-name domain-name
   ```

8. Configure the IP address and prefix length for the router management Ethernet interface, fxp0. fxp0 is an Ethernet management interface that provides a separate out-of-band management network for the router.

   ```
   [edit]
   root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
   ```

9. Configure the IP address of a backup or default routing platform. This device is called the backup router, because it is used only while the routing protocol process is not running. Choose a router that is directly connected to the local routing platform by way of the management interface. The routing platform uses this backup router only when it is booting and only or when the JUNOS routing software (the routing protocol process, rpd) is not running.

   For routing platforms with two Routing Engines, the backup Routing Engine, RE1, uses the backup router as a default gateway after the routing platform boots. This enables you to access the backup Routing Engine. (RE0 is the default master Routing Engine.)

```
[edit]
root@# set system backup-router address
```

10. Configure the IP address of a DNS server. The routing platform uses the DNS name server to translate hostnames into IP addresses.

```
[edit]
root@# set system name-server address
```

11. Set the root password, entering either a clear-text password that the system will encrypt, a password that is already encrypted, or an SSH public key string. For more information about passwords, see "Specifying Plain-Text Passwords" on page 31.

    Choose one of the following:

    a. To enter a clear-text password, use the following command:

```
[edit]
root@# set system root-authentication plain-text-password
New password: type password
Retype new password: retype password
```

    b. To enter a password that is already encrypted, use the following command:

```
[edit]
root@# set system root-authentication encrypted-password
   encrypted-password
```

    c. To enter an SSH public key, use the following command:

```
[edit]
root@# set system root-authentication ssh-rsa key
```

12. Optionally, display the configuration statements:

```
[edit]
root@ show
system {
   host-name hostname;
   domain-name domain.name;
   backup-router address ;
   root-authentication {
      (encrypted-password "password" | public-key);
      ssh-rsa "public-key";
      ssh-dsa "public-key";
   }
   name-server {
      address;
   }
   interfaces {
      fxp0 {
         unit 0 {
            family inet {
               address address ;
            }
```

```
        }
      }
    }
  }
```

13. Commit the configuration, which activates the configuration on the routing platform:

    ```
    [edit]
    root@# commit
    ```

    After committing the configuration, you see the newly configured hostname appear after the username in the prompt—for example, user@host#.

    JUNOS software defaults are now set on the routing platform.

    If you want to configure additional JUNOS software properties at this time, remain in the CLI configuration mode and add the necessary configuration statements. For more information about how to configure additional properties, see "Configuring Software Properties" on page 27 and "System Management" on page 33. You will need to commit your configuration changes to activate them on the routing platform.

14. Exit from the CLI configuration mode.

    ```
    [edit]
    root@ hostname# exit
    root@hostname>
    ```

15. Back up the configuration on the hard drive.

    After you have installed the software on the routing platform, committed the configuration, and are satisfied that the new configuration is successfully running, you should issue the request system snapshot command to back up the new software to the /altconfig file system. If you do not issue the request system snapshot command, the configuration on the alternate boot device will be out of sync with the configuration on the primary boot device.

    The request system snapshot command causes the root file system to be backed up to /altroot, and /config to be backed up to /altconfig. The root and /config file systems are on the routing platform's CompactFlash card, and the /altroot and /altconfig file systems are on the routing platform's hard disk.

**NOTE:** After you issue the request system snapshot command, you cannot return to the previous version of the software, because the running copy and the backup copy of the software are identical.

## *Configuring the JUNOS Software the First Time on a Router with Dual Routing Engines*

If a routing platform has dual Routing Engines, you must initially configure each routing platform independently. The sequence is irrelevant.

Configure the hostnames and addresses of the two Routing Engines using configuration groups at the [edit groups] hierarchy level. Use the reserved configuration group re0 for the Routing Engine in slot 0 and re1 for the Routing Engine in slot 1 to define properties specific to the individual Routing Engines. Configuring re0 and re1 groups enables both Routing Engines to use the same configuration file.

Use the apply-groups statement to reproduce the configuration group information in the main part of the configuration.

The commit synchronize command commits the same configuration on both Routing Engines. The command makes the active or applied configuration the same for both Routing Engines with the exception of the groups, re0 being applied to only RE0 and re1 being applied only to RE1. If you do not synchronize the configurations between two Routing Engines and one of them fails, the routing platform may not forward traffic correctly, because the backup Routing Engine may have a different configuration.

To initially configure a routing platform with dual Routing Engines, follow these steps:

1. Go to "Configuring the JUNOS Software the First Time on a Router with a Single Routing Engine" on page 21 and follow Step 1 through Step 5 to initially configure the backup Routing Engine.
2. Instead of Step 6 and Step 8 in "Configuring the JUNOS Software the First Time on a Router with a Single Routing Engine" on page 21, configure a hostname for each Routing Engine and an IP address for each fxp0 management Ethernet interface, as follows:

   ```
   [edit]
   root@# edit groups
   [edit groups]
   root@# set re0 system host-name router1
   root@# set re0 interfaces fxp0 unit 0 family inet address 10.10.10.1/24
   root@# set re0 system host-name router2
   root@# set re1 interfaces fxp0 unit 0 family inet address 10.10.10.2/24
   ```

3. Configure the routing platform's domain name:

   ```
   [edit]
   root@# set system domain-name domain-name
   ```

4. Set the loopback interface address for each Routing Engine.

   ```
   [edit groups]
   root@# set re0 interfaces lo0 unit 0 family inet address 2.2.2.1/32
   root@# set re1 interfaces lo0 unit 0 family inet address 2.2.2.2/32
   ```

5. Configure the apply-groups statement to reproduce the configuration group information to the main part of the configuration.

   ```
   [edit groups]
   root@# top
   [edit]
   root@# set apply-groups [re0 re1]
   ```

6. Configure Routing Engine redundancy:

```
[edit]
root@# set chassis redundancy routing-engine 0 master
root@# set chassis redundancy routing-engine 1 backup
root@# set chassis redundancy routing-engine graceful-switchover
```

7. Save the configuration change on both Routing Engines:

```
[edit]
user@host> commit synchronize
root@#
```

8. Continue with Step 9 through Step 12 in "Configuring the JUNOS Software the First Time on a Router with a Single Routing Engine" on page 21.

9. After you have installed the new software and are satisfied that it is successfully running, issue the request system snapshot command to back up the new software on both master and backup Routing Engines.

```
{master}
user@host> request system snapshot
```

The root file system is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the routing platform's CompactFlash card, and the /altroot and /altconfig file systems are on the routing platform's hard disk.

**NOTE:** After you issue the request system snapshot command, you cannot return to the previous version of the software, because the running copy and backup copy of the software are identical.

## *JUNOS Software Default Settings That Protect the Router*

The JUNOS software protects against common router security weaknesses with the following default settings:

- The JUNOS software does not forward directed broadcast messages. Directed broadcast services send ping requests from a spoofed source address to a broadcast address and can be used to attack other Internet users. For example, if broadcast ping messages were allowed on the 200.0.0.0/24 network, a single ping request could result in up to 254 responses to the supposed source of the ping. The source would actually become the victim of a denial-of-service (DoS) attack.
- Only console access to the router is enabled by default. Remote management access to the router and all management access protocols, including Telnet, FTP, and SSH (Secure Shell), are disabled by default.
- The JUNOS software does not support the SNMP set capability for editing configuration data. Although the software supports the SNMP set capability for monitoring and troubleshooting the network, this support exposes no known

security issues. (You can configure the software to disable this SNMP set capability.)

- The JUNOS software ignores martian addresses that contain the following prefixes: 0.0.0.0/8, 127.0.0.0/8, 128.0.0.0/16, 191.255.0.0/16, 192.0.0.0/24, 223.255.55.0/24, and 240.0.0.0/4. Martian addresses are reserved host or network addresses about which all routing information should be ignored.

### *Configuring Software Properties*

You configure the JUNOS software using the JUNOS Command Line Interface (CLI). The CLI is described in detail in the *JUNOS CLI User Guide*.

After completing the initial minimal configuration, you can configure software properties. If you configure the software interactively using the CLI, you enter software configuration statements to create a candidate configuration that contains a hierarchy of statements. At any hierarchy level, you generally can enter statements in any order. While you are configuring the software, you can display all or portions of the candidate configuration, and you can insert or delete statements. Any changes you make affect only the candidate configuration, not the active configuration that is running on the router.

The configuration hierarchy logically groups related functions, which results in configuration statements that have a regular, consistent syntax. For example, you configure routing protocols, routing policies, interfaces, and SNMP management in their own separate portions of the configuration hierarchy. For more information about the JUNOS hierarchy, see the *JUNOS Hierarchy and RFC Reference*.

At each level of the hierarchy, you can display a list of the statements available at that level, along with short descriptions of the statements' functions. To have the CLI complete the statement name if it is unambiguous or to provide a list of possible completions, you can type a partial statement name followed by a space or tab.

More than one user can edit a router's configuration simultaneously. All changes made by all users are visible to everyone editing the configuration.

### *Activating a Configuration*

To have a candidate configuration take effect, you commit the changes. At this point, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration, when you commit the candidate configuration, all changes made by all the users take effect.

The CLI always maintains a copy of previously committed versions of the software configuration. If you need to return to a previous configuration, you can do this from within the CLI. For more information, see the *JUNOS CLI User Guide*.

### *Managing Available Disk Space*

A software installation or upgrade may fail if your router has a shortage of disk space. If a disk space error occurs, use one or more of the following options to complete the installation:

- Use the request system storage cleanup command to delete unnecessary files and increase storage space on the router.
- Specify the unlink option when you use the request system software add command to install the JUNOS software:
  - On the J-series platform, the unlink option removes the software package at the earliest opportunity to create enough disk space for the installation to finish.
  - On the M-series, MX-series, and T-series platforms, the unlink option removes the software package after a successful upgrade.
- Download the software packages you need from the Juniper Networks Support Web site, http://www.juniper.net/support/. The download program provides intelligent disk space management to enable installation.

**NOTE:** If you are upgrading the J-series router from a remote location, the installation program automatically checks for enough disk space for the process to finish.

For more information on the request system storage cleanup command and the request system software add command, see the *JUNOS System Basics and Services Command Reference*.

## Using Software Monitoring Tools

The primary method of monitoring and troubleshooting the software, routing protocols, network connectivity, and the router hardware is to enter commands from the CLI. The CLI enables you to display information in the routing tables and routing protocol-specific data, and to check network connectivity using ping and traceroute commands.

The J-Web graphical user interface (GUI) is a Web-based alternative to using CLI commands to monitor, troubleshoot, and manage the router. For more information about J-Web, see “J-Web Package” on page 19.

The JUNOS software includes SNMP software, which allows you to manage routers. The SNMP software consists of an SNMP master agent and a MIB II agent, and supports MIB II SNMP version 1 traps and version 2 notifications, SNMP version 1 Get and GetNext requests, and version 2 GetBulk requests. For more information, see the *JUNOS Network Management Configuration Guide*.

The software also supports tracing and logging operations so that you can track events that occur in the router—both normal router operations and error conditions—and track the packets that are generated by or pass through the router.

Logging operations use a syslog-like mechanism to record system-wide, high-level operations, such as interfaces going up or down and users logging in to or out of the router. Tracing operations record more detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions.

## Router Security

Router security consists of three major elements: physical security of the router, operating system security, and security that can be effected through configuration. Physical security involves restricting access to the router. Exploits that can easily be prevented from remote locations are extremely difficult or impossible to prevent if an attacker can gain access to the router's management port or console. The inherent security of the JUNOS operating system also plays an important role in router security. The JUNOS software is extremely stable and robust. The JUNOS software also provides features to protect against attacks, allowing you to configure the router to minimize vulnerabilities.

This section discusses some JUNOS software features available to improve router security:



### *Router Access*

When you first install the JUNOS software, all remote access to the router is disabled, thereby ensuring that remote access is possible only if deliberately enabled by an authorized user. You can establish remote communication with a router in one of the following ways:

- Out-of-band management—Allows connection to the router through an interface dedicated to router management. Juniper Networks routing platforms support out-of-band management with a dedicated management Ethernet interface (fxp0), as well as EIA-232 console and auxiliary ports. The management Ethernet interface connects directly to the Routing Engine. No transit traffic is allowed through this interface, providing complete separation of customer and management traffic and ensuring that congestion or failures in the transit network do not affect the management of the router.
- Inband management—Allows connection to the routers using the same interfaces through which customer traffic flows. Although this approach is simple and requires no dedicated management resources, it has some disadvantages:
  - Management flows and transit traffic flows are mixed together. Any attack traffic that is mixed with the normal traffic can affect the communication with the router.

- The links between router components might not be totally trustworthy, leading to the possibility of wiretapping and replay attacks.

For management access to the router, the standard ways to communicate with the router from a remote console are with Telnet and SSH. SSH provides secure encrypted communications and is therefore useful for inband router management. Telnet provides unencrypted, and therefore less secure, access to the router. For more information about router access, see "System Management" on page 33.

### *User Authentication*

On a router, you can create local user login accounts to control who can log in to the router and the access privileges they have. A password, either an SSH key or a Message Digest 5 (MD5) password, is associated with each login account. To define access privileges, you create login classes into which you group users with similar jobs or job functions. You use these classes to explicitly define what commands their users are and are not allowed to issue while logged in to the router.

The management of multiple routers by many different personnel can create a user account management problem. One solution is to use a central authentication service to simplify account management, creating and deleting user accounts only on a single, central server. A central authentication system also simplifies the use of one-time password systems such as SecureID, which offer protection against password sniffing and password replay attacks (attacks in which someone uses a captured password to pose as a router administrator).

The JUNOS software supports two protocols for central authentication of users on multiple routers:

- Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).
- RADIUS, a multivendor IETF standard whose features are more widely accepted than those of TACACS+ or other proprietary systems. All one-time-password system vendors support RADIUS. For more information about configuring user access, see "Configuring User Access" on page 61.

The JUNOS software also supports the following authentication methods:

- Internet Protocol Security (IPSec). IPSec architecture provides a security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPSec, the JUNOS software also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs). For more information about IPSec, see the *JUNOS Services Interfaces Configuration Guide*.
- MD5 authentication of MSDP peering sessions. This authentication provides protection against spoofed packets being introduced into a peering session. For more information about SNMPv3, see the *JUNOS Multicast Protocols Configuration Guide*.
- SNMPv3 authentication and encryption. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model

(VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules. For more information about SNMPv3, see the *JUNOS Network Management Configuration Guide*.

### Specifying Plain-Text Passwords

The JUNOS software has special requirements when you create plain-text passwords on a routing platform. The default requirements for plain-text passwords are as follows:

- The password must be between 6 and 128 characters long.
- You can include uppercase letters, lowercase letters, numbers, punctuation marks, and any of the following special characters:
  ! @ # $ % ^ & * , + = < > : ;
  Control characters are not recommended.
- The password must contain at least one change of case or character class.

You can change the requirements for plain-text passwords.

You can include the plain-text-password statement at the following hierarchy levels:

- [edit system diag-port-authentication]
- [edit system pic-console-authentication]
- [edit system root-authentication]
- [edit system login user *username* authentication]

For more information about how to create plain-text passwords, see "Configuring Special Requirements for Plain-Text Passwords" on page 55.

### Routing Protocol Security Features

The main task of a router is to forward user traffic toward its intended destination based on the information in the router's routing and forwarding tables. You can configure routing policies that define the flows of routing information through the network, controlling which routes the routing protocols place in the routing tables and which routes they advertise from the tables. You can also use routing policies to change specific route characteristics, change the BGP route flap-damping values, perform per-packet load balancing, and enable class of service (CoS).

Attackers can send forged protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which can degrade the functionality of the router. To prevent such attacks, you must ensure that routers form routing protocol peering or neighboring relationships with trusted peers. One way to do this is by authenticating routing protocol messages. The JUNOS BGP, IS-IS, OSPF, RIP, and RSVP protocols support HMAC-MD5 authentication, which uses a secret key combined with the data being protected to compute a hash. When the protocols send messages, the computed hash is transmitted with the data. The receiver uses the matching key to validate the message hash.

The JUNOS software supports the IPSec security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. The JUNOS software also supports IKE, which defines mechanisms for key generation and exchange, and manages SAs.

### Firewall Filters

Firewall filters allow you to control packets transiting the router to a network destination and packets destined for and sent by the router. You can configure firewall filters to control which data packets are accepted on and transmitted from the physical interfaces, and which local packets are transmitted from the physical interfaces and the Routing Engine. Firewall filters provide a means of protecting your router from excessive traffic. Firewall filters that control local packets can also protect your router from external aggressions, such as DoS attacks.

To protect the Routing Engine, you can configure a firewall filter only on the router's loopback interface. Adding or modifying filters for each interface on the router is not necessary. You can design firewall filters to protect against ICMP and Transmission Control Protocol (TCP) connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine. For more information about firewall filters, see the *JUNOS Policy Framework Configuration Guide*.

### Auditing for Security

The JUNOS software logs significant events that occur on the router and within the network. Although logging itself does not increase security, you can use the system logs to monitor the effectiveness of your security policies and router configurations. You can also use the logs when reacting to a continued and deliberate attack as a means of identifying the source address, router, or port of the attacker's traffic. You can configure the logging of different levels of events, from only critical events to all events, including informational events. You can then inspect the contents of the system log files either in real time or later.

Debugging and troubleshooting are much easier when the timestamps in the system log files of all routers are synchronized, because events that span the network might be correlated with synchronous entries in multiple logs. The JUNOS software supports the Network Time Protocol (NTP), which you can enable on the router to synchronize the system clocks of routers and other networking equipment. By default, NTP operates in an unauthenticated mode. You can configure various types of authentication, including an HMAC-MD5 scheme. For more information about system logging, see "System Logging Configuration Statements" on page 109 and the *JUNOS System Log Messages Reference*.

## Part 2
# System Management

Chapter 3

# System Management Overview

The JUNOS software provides a variety of parameters that allow you to configure system management functions, including the router's hostname, address, and domain name; the addresses of Domain Name System (DNS) servers; user login accounts, including user authentication and the root-level user account; time zones and Network Time Protocol (NTP) properties; and properties of the router's auxiliary and console ports.

This chapter discusses the following topics, which provide background information related to configuring system management:



## Specifying IP Addresses, Network Masks, and Prefixes

Many statements in the JUNOS software configuration include an option to specify an IP address or route prefix. In this manual, this option is represented in one of the following ways:

- *network/prefix-length*—Network portion of the IP address, followed by a slash and the destination prefix length (previously called the subnet mask). For example, 10.0.0.1/8.
- *network*—IP address. For example, 10.0.0.2.
- *destination-prefix/prefix-length*—Route prefix, followed by a slash and the destination prefix length. For example, 192.168.1.10/32.

You enter all IP addresses in classless mode. You can enter the IP address with or without a prefix length, in standard dotted notation (for example, 1.2.3.4), or hexadecimal notation as a 32-bit number in network-byte order (for example, 0x01020304). If you omit any octets, they are assumed to be zero. Specify the prefix length as a decimal number in the range from 1 through 32.

## Specifying Filenames and URLs

In some command-line interface (CLI) commands and configuration statements—including file copy, file archive, load, save, set system login user *username* authentication *load-key-file*, and request system software add—you can include a filename. On a routing matrix, you can include chassis information; for example, lcc0, lcc0-re0, or lcc0-re1, as part of the filename. A routing matrix is a multichassis architecture composed of one TX Matrix platform, to which you can connect from one to four T640 routing nodes. For more information about the routing matrix, see "TX Matrix Platform and T640 Routing Node Configuration Guidelines" on page 779 and the *TX Matrix Platform Hardware Guide*.

You can specify a filename or URL in one of the following ways:

- *filename*—File in the user's current directory on the local CompactFlash card. You can use wildcards to specify multiple source files or a single destination file. Wildcards are not supported in Hypertext Transfer Protocol (HTTP) or FTP.

**NOTE:** Wildcards are supported only by the file (compare | copy | delete | list | rename | show) commands. When you issue the file show command with a wildcard, it must resolve to one filename.

- */path/filename*—File on the local flash disk.
- /var/*filename* or /var/*path/filename*—File on the local hard disk. You can also specify a file on a local Routing Engine for a specific T640 routing node on a routing matrix:

```
user@host> file delete lcc0-re0:/var/tmp/junk
```

- a:*filename* or a:*path/filename*—File on the local. The default path is / (the root-level directory). The removable media can be in MS-DOS or UNIX (UFS) format.
- *hostname:/path/filename*, *hostname*:*filename*, *hostname*:*path/filename*, or "scp://*hostname/path/filename*"—File on an scp/ssh client. This form is not available in the worldwide version of the JUNOS software. The default path is the user's home directory on the remote system. You can also specify *hostname* as *username@hostname*.
- ftp://*hostname/path/filename*—File on an FTP server. You can also specify *hostname* as *username@hostname* or *username*:*password@hostname*. The default path is the user's home directory. To specify an absolute path, the path must start with %2F; for example, ftp://*hostname*/%2F*path/filename*. To have the system prompt you for the password, specify prompt in place of the password. If a password is required, and you do not specify the password or prompt, an error message is displayed:

```
user@host> file copy ftp://username@ftp.hostname.net//filename

file copy ftp.hostname.net: Not logged in.

user@host> file copy ftp://username:prompt@ftp.hostname.net//filename
```

```
Password for username@ftp.hostname.net:
```

- http://*hostname*/*path*/*filename*—File on an HTTP server. You can also specify *hostname* as *username*@*hostname* or *username*:*password*@*hostname*. If a password is required and you omit it, you are prompted for it.
- re0:/*path*/*filename* or re1:/*path*/*filename*—File on a local Routing Engine. You can also specify a file on a local Routing Engine for a specific T640 routing node on a routing matrix:

```
user@host> show log lcc0-re1:chassisd
```

## Directories on the Router

JUNOS software files are stored in the following directories on the router:

- /altconfig—When you back up the currently running and active file system partitions on the router to standby partitions using the request system snapshot command, the /config directory is backed up to /altconfig. Normally, the /config directory is on the CompactFlash card and /altconfig is on the hard disk.
- /altroot—When you back up the currently running and active file system partitions on the router to standby partitions using the request system snapshot command, the root file system (/) is backed up to /altroot. Normally, the root directory is on the CompactFlash card and /altroot is on the hard disk.
- /config—This directory is located on the primary boot device, that is, on the from which the router booted (generally the CompactFlash card, device wd0). This directory contains the current operational router configuration and the last three committed configurations, in the files juniper.conf, juniper.conf.1, juniper.conf.2, and juniper.conf.3, respectively.
- /var—This directory is always located on the hard disk (device wd2). It contains the following subdirectories:
  - /var/home—Contains users' home directories, which are created when you create user access accounts. For users using SSH authentication, their .ssh file, which contains their SSH key, is placed in their home directory. When a user saves or loads a configuration file, that file is loaded from their home directory unless the user specifies a full pathname.
  - /var/db/config—Up to six additional previous versions of committed configurations, which are stored in the files juniper.conf.4 through juniper.conf.9.
  - /var/log—Contains system log and tracing files.
  - /var/tmp—Contains core files. The software saves up to five core files, numbered from 0 through 4. File number 0 is the oldest core file and file number 4 is the newest core file. To preserve the oldest core files, the software overwrites the newest core file, number 4, with any subsequent core file.

Each router ships with removable media (device wfd0) that contains a backup copy of the JUNOS software.

## Tracing and Logging Operations

Tracing and logging operations allow you to track events that occur in the router—both normal router operations and error conditions—and to track the packets that are generated by or passed through the router. The results of tracing and logging operations are placed in files in the /var/log directory on the router.

The JUNOS software provides an option to do remote tracing for specific processes, which greatly reduces use of the router's internal storage for tracing and is analogous to remote system logging. You configure remote tracing system-wide using the tracing statement under the [edit system] hierarchy. By default, remote tracing is not configured. You can disable remote tracing for specific processes using the no-remote-trace statement at the [edit <process-name> traceoptions] hierarchy. This feature does not alter local tracing functionality in any way; whereby logging files are stored on the router.

The JUNOS software supports remote tracing for the following processes:

- chassisd—chassis-control process
- eventd—event-processing process
- cosd—class-of-service process
- spd—adaptive-services process

Logging operations use a system logging mechanism similar to the UNIX syslogd utility to record systemwide, high-level operations, such as interfaces going up or down and users logging in to or out of the router. You configure these operations by using the syslog statement at the [edit system] hierarchy level, as described in "Configuring System Log Messages" on page 109, and by using the options statement at the [edit routing-options] hierarchy level, as described in the *JUNOS Routing Protocols Configuration Guide*.

Tracing operations record more detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions. You configure tracing operations using the traceoptions statement. You can define tracing operations in different portions of the router configuration:

- Global tracing operations—Define tracing for all routing protocols. You define these tracing operations at the [edit routing-options] hierarchy level of the configuration. For more information, see the *JUNOS Routing Protocols Configuration Guide*.
- Protocol-specific tracing operations—Define tracing for a specific routing protocol. You define these tracing operations in the [edit protocol] hierarchy when configuring the individual routing protocol. Protocol-specific tracing operations override any equivalent operations that you specify in the global traceoptions statement. If there are no equivalent operations, they supplement the global tracing options. If you do not specify any protocol-specific tracing, the routing protocol inherits all the global tracing operations.

- Tracing operations within individual routing protocol entities—Some protocols allow you to define more granular tracing operations. For example, in Border Gateway Protocol (BGP), you can configure peer-specific tracing operations. These operations override any equivalent BGP-wide operations or, if there are no equivalents, supplement them. If you do not specify any peer-specific tracing operations, the peers inherit, first, all the BGP-wide tracing operations and, second, the global tracing operations.
- Interface tracing operations—Define tracing for individual router interfaces and for the interface process itself. You define these tracing operations at the [edit interfaces] hierarchy level of the configuration as described in the *JUNOS Network Interfaces Configuration Guide*.
- Remote tracing—To enable system-wide remote tracing, include the destination-override syslog host statement at the [edit system tracing] hierarchy level. This specifies the remote host running the system log process (syslogd), which collects the traces. Traces are written to one or more files on the remote host per the syslogd configuration in /etc/syslog.conf. By default remote tracing is *not* configured.

  To override the system-wide remote tracing configuration for a particular process, include the no-remote-trace statement at the [edit *process-name* traceoptions] hierarchy. When no-remote-trace is enabled, the process does local tracing.

  To collect traces, use the local0 facility as the selector in /etc/syslog.conf on the remote host. To separate traces from various processes into different files, include the process name or trace-file name if it is specified at the [edit *process-name* traceoptions file] hierarchy level, in the program field in /etc/syslog.conf. If your syslog server supports parsing hostname and program-name, then you can separate traces from the various processes. For more information, issue the man syslog.conf command on the remote host.

## Configuring Protocol Authentication

Some interior gateway protocols (IGPs)—Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP)—and Resource Reservation Protocol (RSVP) allow you to configure an authentication method and password. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface. The following authentication methods are supported:

- Simple authentication (IS-IS, OSPF, and RIP)—Uses a simple text password. The receiving router uses an authentication key (password) to verify the packet. Because the password is included in the transmitted packet, this method of authentication is relatively insecure. We recommend that you not use this authentication method.
- MD5 and HMAC-MD5 (IS-IS, OSPF, RIP, and RSVP)—Message Digest 5 (MD5) creates an encoded checksum that is included in the transmitted packet. HMAC-MD5, which combines HMAC authentication with MD5, adds the use of an iterated cryptographic hash function. With both types of authentication, the receiving router uses an authentication key (password) to verify the packet. HMAC-MD5 authentication is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

In general, authentication passwords are text strings consisting of a maximum of 16 or 255 letters and digits. Characters can include any ASCII strings. If you include spaces in a password, enclose all characters in quotation marks (“ ”).

JUNOS-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If JUNOS-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

## Configuring User Authentication

The JUNOS software supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and 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 router.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router using telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router, and the server runs on a remote network system.

You can configure the router to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the JUNOS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

Chapter 4

# System Management Configuration Statements

To configure system management, you can include the following statements in the configuration:

```
system {
    accounting {
        events [ login change-log interactive-commands ];
        destination {
            radius {
                server {
                    server-address {
                        accounting-port port-number;
                        retry number;
                        secret password;
                        source-address address;
                        timeout seconds;
                    }
                }
            }
            tacplus {
                server {
                    server-address {
                        port port-number;
                        secret password;
                        single-connection;
                        timeout seconds;
                    }
                }
            }
        }
    }
    archival {
        configuration {
            archive-sites {
                ftp://<username>:<password>@<host>:<port>/<url-path>;
                ftp://<username>:<password>@<host>:<port>/<url-path>;
            }
            transfer-interval interval;
            transfer-on-commit;
        }
    }
    arp {
```

```
    passive-learning;
    aging-timer minutes;
}
authentication-order [ authentication-methods ];
backup-router address <destination destination-address>;
commit synchronize;
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
dump-device (compact-flash | remove-compact | usb);
diag-port-authentication (encrypted-password "password" | plain-text-password);
domain-name domain-name;
domain-search [ domain-list ];
host-name hostname;
inet6-backup-router address <destination destination-address>;
internet-options {
    tcp-mss mss-value;
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit {
        bucket-size bucket-size;
        packet-rate packet-rate;
    }
    icmpv6-rate-limit {
        bucket-size bucket-size;
        packet-rate packet-rate;
    }
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout;
    no-tcp-rfc1323;
    no-tcp-rfc1323-paws;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit <upper-limit>;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
}
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
login {
    announcement text;
    class class-name {
        allow-commands "regular-expression";
        allow-configuration "regular-expression";
        deny-commands "regular-expression";
        deny-configuration "regular-expression";
```

```
        idle-timeout minutes;
        login-tip;
        permissions [ permissions ];
    }
    message text;
    password (Login) {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication {
            (encrypted-password "password" | plain-text-password);
            ssh-rsa "public-key";
            ssh-dsa "public-key";
        }
    }
}
login-tip number;
mirror-flash-on-disk;
name-server {
    address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
    authentication-key key-number type type value password;
    boot-server (NTP) address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    source-address source-address;
    server address <key key-number> <version value> <prefer>;
    trusted-key [ key-numbers ];
}
ports {
    auxiliary {
        type terminal-type;
    }
    pic-console-authentication {
        encrypted-password encrypted-password;
        plain-text-password;
```

```
        console {
            insecure;
            log-out-on-disconnect;
            type terminal-type;
            disable;
        }
    }
    processes {
        process–name (enable | disable) failover (alternate-media | other-routing-engine);
        timeout seconds;
    }
}
radius-server server-address {
    port port-number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
}
radius-options {
    password-protocol mschap-v2;
    }
    attributes {
        nas-ip-address ip-address;
root-authentication {
    (encrypted-password “password” | plain-text-password);
    ssh-rsa “public-key”;
    ssh-dsa “public-key”;
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
scripts {
    commit {
        allow-transients;
        file filename.xsl {
            optional;
            refresh;
            refresh-from url;
            source url;
        }
        traceoptions {
            file filename <files number> <size size> <match regular-expression>;
            flag flag;
    }
}
services {
    finger {
        <connection-limit limit>;
        <rate-limit limit>;
    }
    flow-tap-dtcp {
        ssh {
            <connection-limit limit>;
            <rate-limit limit>;
        }
    }
```

```
    ftp {
        <connection-limit limit>;
        <rate-limit limit>;
    }
    service-deployment {
        servers server-address {
            port port-number;
        }
        source-address source-address;
    }
    ssh {
        root-login (allow | deny | deny-password);
        protocol-version [v1 v2];
        <connection-limit limit>;
        <rate-limit limit>;
    }
    telnet {
        <connection-limit limit>;
        <rate-limit limit>;
    }
    web-management {
        http {
            interfaces [ interface-names ];
            port port;
        }
        https {
            interfaces [ interface-names ];
            local-certificate name;
            port port;
        }
        limits {
            active-child-process [ process-limit ];
        }
        session {
            idle-timeout [ minutes ];
            session-limit [ session-limit ];
        }
    }
    xnm-clear-text {
        <connection-limit limit>;
        <rate-limit limit>;
    }
    xnm-ssl {
        <connection-limit limit>;
        local-certificate name;
        <rate-limit limit>;
    }
}
static-host-mapping {
    hostname {
        alias [ alias ];
        inet [ address ];
        sysid system-identifier;
    }
}
syslog {
```

```
        archive {
            files number;
            size size;
            (world-readable | no-world-readable);
        }
        console {
            facility severity;
        }
        file filename {
            facility severity;
            explicit-priority;
            match "regular-expression";
            structured-data;
            archive {
                files number;
                size size;
                (world-readable | no-world-readable);
            }
        }
        host (hostname | other-routing-engine | scc-master) {
            facility severity;
            explicit-priority;
            facility-override facility;
            log-prefix string;
            match "regular-expression";
        }
        source-address source-address;
        time-format (year | millisecond | year millisecond);
        user (username | *) {
            facility severity;
            match "regular-expression";
        }
    }
    tacplus-options {
        service-name service-name;
        (no-cmd-attribute-value | exclude-cmd-attribute);
    }
    tacplus-server server-address {
        secret password;
        single-connection;
        source-address source-address;
        timeout seconds;
    }
    time-zone (GMT<(+ | –)hour-offset> | time-zone);
}
    tracing{
        destination-override {
        syslog host ;
        }
    }
```

Chapter 5

# Configuring Basic System Management

This chapter discusses the following topics:



## Configuring the Router's Name and Addresses

This section includes the following topics:



For an example of how to configure a router's name, IP address, and system identifier, see "Example: Configuring a Router's Name, IP Address, and System ID" on page 48.

### *Configuring the Router's Name*

To configure the router's name, include the host-name statement at the [edit system] hierarchy level:

```
[edit system]
host-name hostname;
```

The router's name value must be less than 256 characters.

### Mapping the Router's Name to IP Addresses

To map a router's hostname to one or more IP addresses, include the inet statement at the [edit system static-host-mapping *hostname*] hierarchy level:

```
[edit system]
static-host-mapping {
   hostname {
      inet [ addresses ];
      alias [ aliases ];
   }
}
```

*hostname* is the name specified by the host-name statement at the [edit system] hierarchy level.

For each host, you can specify one or more aliases.

### Configuring an ISO System Identifier

For IS-IS to operate on the router, you must configure a system identifier (system ID). The system identifier is commonly the media access control (MAC) address or the IP address expressed in binary-coded decimal (BCD). For more information, see the *JUNOS Routing Protocols Configuration Guide*.

To configure an International Organization for Standardization (ISO) system ID, include the sysid statement at the [edit system static-host-mapping *hostname*] hierarchy level:

```
[edit system]
static-host-mapping {
   hostname {
      sysid system-identifier;
   }
}
```

*hostname* is the name specified by the host-name statement at the [edit system] hierarchy level.

*system-identifier* is the ISO system identifier. It is the 6-byte system ID portion of the IS-IS network service access point (NSAP). We recommend that you use the host's IP address represented in BCD format. For example, the IP address 192.168.1.77 is 1921.6800.1077 in BCD.

### Example: Configuring a Router's Name, IP Address, and System ID

Configure the router's name, map the name to an IP address and alias, and configure a system identifier:

```
[edit]
user@host# set system host-name router-sj1
[edit]
user@host# set system static-host-mapping router-sj1 inet 192.168.1.77
```

```
[edit]
user@host# set system static-host-mapping router-sj1 alias sj1
[edit]
user@host# set system static-host-mapping router-sj1 sysid 1921.6800.1077
[edit]
user@host# show
system {
   host-name router-sj1;
   static-host-mapping {
      router-sj1 {
         inet 192.168.1.77;
         alias sj1;
         sysid 1921.6800.1077;
      }
   }
}
```

## Configuring the Router's Domain Name

For each router, you should configure the name of the domain in which the router is located. This is the default domain name that is appended to hostnames that are not fully qualified. To configure the domain name, include the domain-name statement at the [edit system] hierarchy level:

```
[edit system]
domain-name domain-name;
```

### *Example: Configuring the Router's Domain Name*

Configure the router's domain name:

```
[edit]
user@host# set system domain-name company.net
[edit]
user@host# show
system {
   domain-name company.net;
}
```

## Configuring Which Domains to Search

If your router is included in several different domains, you can configure those domain names to be searched.

To configure more than one domain to be searched, include the domain-search statement at the [edit system] hierarchy level:

```
[edit system]
domain-search [ domain-list ];
```

The domain list can contain up to 6 domain names, with a total of up to 256 characters.

### *Example: Configuring Which Domains to Search*

Configure two domains to be searched:

```
[edit system]
domain-search [ domainone.net domainonealternate.com ]
```

## Configuring a DNS Name Server

To have the router resolve hostnames into addresses, you must configure one or more Domain Name System (DNS) name servers by including the name-server statement at the [edit system] hierarchy level:

```
[edit system]
name-server {
   address;
}
```

### *Example: Configuring a DNS Name Server*

Configure two DNS name servers:

```
[edit]
user@host# set system name-server 192.168.1.253
[edit]
user@host# set system name-server 192.168.1.254
[edit]
user@host# show
system {
   name server {
      192.168.1.253;
      192.168.1.254;
   }
}
```

## Configuring a Backup Router

When the router is booting, the routing protocol process (rpd) is not running; therefore, the router has no static or default routes. To allow the router to boot and to ensure that the router is reachable over the network if the routing protocol process fails to start properly, you configure a backup router (running IP version 4 [IPv4] or IP version 6 [IPv6]), which is a router that is directly connected to the local router (that is, on the same subnet).

To configure a backup router running IPv4, include the backup-router statement at the [edit system] hierarchy level:

```
[edit system]
backup-router address <destination destination-address>;
```

To configure a backup router running IPv6, include the inet6-backup-router statement at the [edit system] hierarchy level:

```
[edit system]
inet6-backup-router "address <destination destination-address>";
```

By default, all hosts (default route) are reachable through the backup router. To eliminate the risk of installing a default route in the forwarding table, include the destination option, specifying an address that is reachable through the backup router. Specify the address in the format *network/mask-length* so that the entire network is reachable through the backup router.

When the routing protocols start, the address of the backup router is removed from the local routing and forwarding tables. To have the address remain in these tables, configure a static route for that address by including the static statement at the [edit routing-options] hierarchy level.

### *Example: Configuring a Backup Router Running IPv4*

Configure a backup router and have its address remain in the routing and forwarding tables:

```
[edit]
system {
   backup-router 192.168.1.254 destination 208.197.1.0/24;
}
routing-options {
   static {
      route 208.197.1.0/24 {
         next-hop 192.168.1.254;
         retain;
      }
   }
}
```

### *Example: Configuring a Backup Router Running IPv6*

Configure a backup router running IPv6 and have its address remain in the routing and forwarding tables:

```
[edit]
system {
   backup-router 8:3::1 destination abcd::/48;
}
routing-options {
   rib inet6.0 {
      static {
         route abcd::/48 {
            next-hop 8:3::1;
            retain;
         }
      }
   }
}
```

## Configuring Flash Disk Mirroring

You can direct the hard disk to automatically mirror the contents of the CompactFlash card. When you include the mirror-flash-on-disk statement, the hard disk maintains a synchronized mirror copy of the CompactFlash card contents. Data written to the CompactFlash is simultaneously updated in the mirrored copy of the hard disk. If the CompactFlash card fails to read data, the hard disk automatically retrieves its mirrored copy of the CompactFlash card. This feature is not available on the J-series routers.

**CAUTION:** We recommend that you disable flash disk mirroring when you upgrade or downgrade the router.

You cannot issue the request system snapshot command while flash disk mirroring is enabled.

To configure the mirroring of the CompactFlash to the hard disk, include the mirror-flash-on-disk statement at the [edit system] hierarchy level:

```
[edit system]
mirror-flash-on-disk;
```

**NOTE:** After you have enabled or disabled the mirror-flash-on-disk statement, you must reboot the router for your changes to take effect. To reboot, issue the request system reboot command.

## Configuring the System Location

To configure the physical location of the system, include the location statement at the [edit system] hierarchy level:

```
[edit system]
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
```

You can configure the following options:

- altitude *feet*—Number of feet above sea level.
- building *name*—Name of the building, 1 to 28 characters in length. If the string contains spaces, enclose it in quotation marks (" ").
- country-code *code*—Two-letter country code.
- floor *number*—Floor in the building.
- hcoord *horizontal-coordinate*—Bellcore Horizontal Coordinate.
- lata *service-area*—Long-distance service area.
- latitude *degrees*—Latitude in degree format.
- longitude *degrees*—Longitude in degree format.
- npa-nxx *number*—First six digits of the phone number (area code and exchange).
- postal-code *postal-code*—Postal code.
- rack *number*—Rack number.
- vcoord *vertical-coordinate*—Bellcore Vertical Coordinate.

## Configuring the Root Password

The JUNOS software is preinstalled on the router. When the router is powered on, it is ready to be configured. Initially, you log in to the router as the user "root" with no password.

**NOTE:** If you configure a blank password using the encrypted-password statement at the [edit system root-authentication] hierarchy level for root authentication, you will be able to commit a configuration, but you will *not* be able to login as superuser and get root level access to the router.

After you log in, you should configure the root (superuser) password by including the root-authentication statement at the [edit system] hierarchy level:

```
[edit system]
root-authentication {
   (encrypted-password "password"| plain-text-password);
   ssh-dsa "public-key";
   ssh-rsa "public-key";
}
```

If you configure the plain-text-password option, you are prompted to enter and confirm the password:

```
[edit system]
user@host# set root-authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

To load an SSH key file, enter the load-key-file command. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys.

You can also configure SSH RSA keys and SSH DSA keys to authenticate root logins. You can configure more than one public RSA or DSA key for SSH authentication of root logins as well as for user accounts. When a user logs in as root, the public keys are referenced to determine whether the private key matches any of them. For more information about how to configure user accounts, see "Configuring User Accounts" on page 72. For an example of how to configure SSH public keys for root authentication, see "Example: Configuring SSH Authentication for Root Logins" on page 55.

If you load the SSH keys file, the contents of the file are copied into the configuration immediately after you enter the load-key-file statement. To view the SSH keys entries, use the configuration mode show command. For example:

```
[edit system]
user@host# set root-authentication load-key-file my-host:.ssh/identity.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
   ssh-rsa "1024 35 9727638204084251055468226757249864241630322
      207404962528390382038690141584534964170019610608358722961
      563475749182736033612764418742659468932077391083448101 2
      683125957722625461667999278316123500438660915866283822 48
      974673260566119214895398139655615637862119403276878065 38
      169602027491641637359132693963440084 43 boojum@juniper.net"; #
      SECRET-DATA
}
```

JUNOS-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If JUNOS-FIPS is installed on the router, you cannot configure passwords unless they meet this standard. If you use the encrypted-password option, then a null-password (empty) is not permitted.

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

### *Example: Configuring the Root Password*

Configure an encrypted password:

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

```
[edit]
user@host# set system root-authentication encrypted-password
   "$1$14c5.$sBopasddsdfs0"
[edit]
```

```
user@host# show
system {
    root-authentication {
        encrypted-password "$1$14c5.$sBopasddsdfs0";
    }
}
```

Configure a plain-text password:

```
[edit]
user@host# set system root-authentication plain-text-password
New password: type root password
Retype new password: retype root password
[edit]
user@host# show
system {
    root-authentication {
        encrypted-password "$1$14c5.$sBopasddsdfs0";
    }
}
```

### *Example: Configuring SSH Authentication for Root Logins*

In this example, you configure two public DSA keys for SSH authentication of root logins.

```
[edit system]
root-authentication {
    encrypted-password "$1$1wp5tqMX$uy/u5H7OdXTwfWTmeJWXe/";
    ## SECRET-DATA;
    ssh-dsa "2354 95 9304@boojum.per";
    ssh-dsa "0483 02 8362@ecbatana.per";
}
```

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

## Configuring Special Requirements for Plain-Text Passwords

The JUNOS software has special requirements when you create plain-text passwords on a routing platform. Table 9 on page 55 shows the default requirements.

**Table 9: Special Requirements for Plain-Text Passwords**

| JUNOS Software | JUNOS-FIPS |
|---|---|
| The password must be between 6 and 128 characters long. | FIPS passwords must be between 10 and 20 characters in length |

**Table 9: Special Requirements for Plain-Text Passwords** *(continued)*

| JUNOS Software | JUNOS-FIPS |
|---|---|
| You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended. | You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended. |
| Valid passwords must contain at least one change of case or character class. | Passwords must use at least three of the five defined character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). |

JUNOS software supports the following five character classes for plain-text passwords:

- Lowercase letters
- Uppercase letters
- Numbers
- Punctuation
- Special characters: ! @ # $ % ^ & * , + < > : ;

Control characters are not recommended.

To change the requirements for plain-text passwords, include the password statement at the [edit system login] hierarchy level:

```
[edit system login]
password {
    change-type (set-transitions | character-set);
    format (md5 | sha1 | des);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
}
```

These statements apply to plain-text passwords only, not encrypted passwords.

The change-type statement specifies whether the password is checked for the following:

- The total number of character sets used (character-set)
- The total number of character set changes (set-transitions)

For example, the following password:

```
MyPassWd@2
```

has four character sets (uppercase letters, lowercase letters, special characters, and numbers) and seven character set changes (M–y, y–P, P–a, s–W, W–d, d–@, and @–2).

The change-type statement is optional. If change-type is omitted, JUNOS-FIPS plain-text passwords are checked for character sets and JUNOS plain-text passwords are checked for character set changes.

The minimum-changes statement specifies how many character sets or character set changes are required for the password. This statement is optional. If minimum-changes is not specified, character sets are not checked for JUNOS software. If the change-type statement is configured for character-set, then minimum-changes must be 5 or less because JUNOS software only supports 5 character sets.

The format statement specifies the hash algorithm (md5, sha1 or des) for authenticating plain-text passwords. This statement is optional. For JUNOS software, the default format is md5. For JUNOS-FIPS, only sha1 is supported.

The maximum-length statement specifies the maximum number of characters allowed in a password. This statement is optional. By default JUNOS passwords have no maximum; however, only the first 128 characters are significant. JUNOS-FIPS passwords must be 20 characters or less. The range for JUNOS software maximum-length passwords is from 20 to 128 characters.

The minimum-length statement specifies the minimum number of characters required for a password. This statement is optional. By default JUNOS passwords must be at least 6 characters long, and JUNOS-FIPS passwords must be at least 10 characters long. The range is from 6 to 20 characters.

Changes to password requirements do not take effect until the configuration is committed. When requirements change, only newly created, plain-text passwords are checked; existing passwords are not checked against the new requirements.

The default configuration for JUNOS plain-text passwords is:

```
[edit system login]
passwords {
    change-type character-sets;
    format md5;
    minimum-changes 1;
    minimum-length 6;
}
```

The default configuration for JUNOS-FIPS plain-text passwords is:

```
[edit system login]
passwords {
    change-type set-transitions;
    format sha1;
    maximum-length 20;
    minimum-changes 3;
    minimum-length 10;
}
```

### *Example: Configuring Special Requirements for Plain-Text Passwords*

In this example, the minimum password length is set to 12 characters and the maximum length is set to 22 characters.

```
[edit system login]
passwords {
   minimum-length 12;
   maximum-length 22;
}
```

## Configuring Multiple Routing Engines to Synchronize Configurations Automatically

If your router has multiple Routing Engines, you can manually direct one Routing Engine to synchronize its configuration with the others by issuing the commit synchronize command.

To make the Routing Engines synchronize automatically whenever a configuration is committed, include the commit synchronize statement at the [edit system] hierarchy level:

```
[edit system]
commit synchronize;
```

The Routing Engine on which you execute the commit command (requesting Routing Engine) copies and loads its candidate configuration to the other (responding) Routing Engines. All Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on all Routing Engines.

## Compressing the Current Configuration File

By default, the current operational configuration file is compressed, and is stored in the file juniper.conf.gz, in the /config file system, along with the last three committed versions of the configuration. If you have large networks, the current configuration file might exceed the available space in the /config file system. Compressing the current configuration file allows the file to fit in the file system, typically reducing the size of the file by 90 percent. You might want to compress your current operation configuration files when they reach 3 megabytes (MB) in size.

When you compress the current configuration file, the names of the router's configuration files change. To determine the size of the files in the /config file system, issue the file list /config detail command.

**NOTE:** We recommend that you use the default setting (compress the router configuration files) to minimize the amount of disk space that they require.

If you do not want to compress the current operational configuration file, include the no-compress-configuration-files statement at the [edit system] hierarchy level:

```
[edit system]
no-compress-configuration-files;
```

Commit the current configuration file to include the no-compress-configuration-files statement. Commit the configuration again to uncompress the current configuration file:

```
[edit system]
user@host#
user@host# commit
commit complete
user@host# commit
commit complete
```

To compress the current configuration file, include the compress-configuration-files statement at the [edit system] hierarchy level:

```
[edit system]
compress-configuration-files;
```

Commit the current configuration file to include the compression-configuration-files statement. Commit the configuration again to compress the current configuration file:

```
[edit system]
user@host# set compress-configuration-files
user@host# commit
commit complete
user@host# commit
commit complete
```

Chapter 6

# Configuring User Access

This chapter contains information about how to configure user access. For information about how to configure user access by means of SSH, see "Configuring SSH Service" on page 181.



## Defining Login Classes

All users who can log in to the router must be in a login class. With login classes, you define the following:

- Access privileges users have when they are logged in to the router
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

You can define any number of login classes. You then apply one login class to an individual user account, as described in "Configuring User Accounts" on page 72.

To define a login class and its access privileges, include the **class** statement at the [edit system login] hierarchy level:

```
[edit system login]
class class-name {
    allow-commands "regular-expression";
    allow-configuration "regular-expression";
    deny-commands "regular-expression";
    deny-configuration "regular-expression";
    idle-timeout minutes;
    permissions [ permissions ];
}
```

Use *class-name* to name the login class. The software contains a few predefined login classes, which are listed in Table 10 on page 62. The predefined login classes cannot be modified.

**Table 10: Default System Login Classes**

| Login Class | Permission Flag Set |
|---|---|
| operator | clear, network, reset, trace, view |
| read-only | view |
| super-user | all |
| unauthorized | None |

**NOTE:** You cannot modify a predefined login class name. If you issue the set command on a predefined class name, the JUNOS software will append -local to the login class name. The following message also appears:

warning: '<*class-name*>' is a predefined class name; changing to '<*class-name*>-local'

**NOTE:** You cannot issue the rename or copy command on a predefined login class. Doing so results in the following error message:

error: target '<*class-name*>' is a predefined class

For each login class, you can do the following:

- Configuring Access Privilege Levels on page 62
- Denying or Allowing Individual Commands on page 65
- Configuring the Timeout Value for Idle Login Sessions on page 71
- Configuring Tips on page 72

## *Configuring Access Privilege Levels*

Each top-level command-line interface (CLI) command and each configuration statement has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges. The privilege level for each command and statement is listed in the summary chapter of the part in which that command or statement is described. The access privileges for each login class are defined by one or more *permission flags*.

To configure access privilege levels, include the permissions statement at the [edit system login class *class-name*] hierarchy level:

[edit system login class *class-name*]
permissions [ *permissions* ];

*permissions* specifies one or more of the permission flags listed in Table 11 on page 63. Permission flags are not cumulative, so for each class you must list all the permission flags needed, including view to display information and configure to enter configuration mode. Two forms for the permissions control the individual parts of the configuration:

- "Plain" form—Provides read-only capability for that permission type. An example is interface.
- Form that ends in -control—Provides read and write capability for that permission type. An example is interface-control.

**Table 11: Login Class Permission Flags**

| Permission Flag | Description |
|---|---|
| access | Can view the access configuration in configuration mode using the show configuration operational mode command. |
| access-control | Can view and configure access information at the [edit access] hierarchy level. |
| admin | Can view user account information in configuration mode and with the show configuration command. |
| admin-control | Can view user accounts and configure them at the [edit system login] hierarchy level. |
| all | Has all permissions. |
| clear | Can clear (delete) information learned from the network that is stored in various network databases using the clear commands. |
| configure | Can enter configuration mode using the configure command. |
| control | Can perform all control-level operations—all operations configured with the -control permission flags. |
| field | Reserved for field (debugging) support. |
| firewall | Can view the firewall filter configuration in configuration mode. |
| firewall-control | Can view and configure firewall filter information at the [edit firewall] hierarchy level. |
| floppy | Can read from and write to the removable media. |
| flow-tap | Can view the flow-tap configuration in configuration mode. |
| flow-tap control | Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the [edit services flow-tap] hierarchy level. |
| flow-tap-operation | Can make flow-tap requests to the router. For example, a Dynamic Tasking Control Protocol (DTCP) client must authenticate itself to JUNOS as an administrative user. That account must have flow-tap-operation permission.<br><br>**NOTE:** flow-tap operation is not included in the all permission. |
| interface | Can view the interface configuration in configuration mode and with the show configuration operational mode command. |

**Table 11: Login Class Permission Flags** *(continued)*

| Permission Flag | Description |
|---|---|
| interface-control | Can view the interface configuration in configuration mode and with the show configuration operational mode command. |
| maintenance | Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell using the su root command, and can halt and reboot the router using the request system commands. |
| network | Can access the network by entering the ping, SSH, telnet, and traceroute commands. |
| reset | Can restart software processes using the restart command and can configure whether software processes are enabled or disabled at the [edit system processes] hierarchy level. |
| rollback | Can use the rollback command to return to a previously committed configuration other than the most recently committed one. |
| routing | Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes. |
| routing-control | Can view general routing, routing protocol, and routing policy configuration information and configure general routing at the [edit routing-options] hierarchy level, routing protocols at the [edit protocols] hierarchy level, and routing policy at the [edit policy-options] hierarchy level. |
| secret | Can view passwords and other authentication keys in the configuration. |
| secret-control | Can view passwords and other authentication keys in the configuration and can modify them in configuration mode. |
| security | Can view security configuration in configuration mode and with the show configuration operational mode command. |
| security-control | Can view and configure security information at the [edit security] hierarchy level. |
| shell | Can start a local shell on the router by entering the start shell command. |
| snmp | Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes. |
| snmp-control | Can view SNMP configuration information and modify SNMP configuration at the [edit snmp] hierarchy level. |
| system | Can view system-level information in configuration and operational modes. |
| system-control | Can view system-level configuration information and configure it at the [edit system] hierarchy level. |
| trace | Can view trace file settings in configuration and operational modes. |
| trace-control | Can view trace file settings and configure trace file properties. |
| view | Can use various commands to display current systemwide, routing table, and protocol-specific values and statistics. Cannot view secret configuration. |

### Example: Configuring Access Privilege Levels

Create two access privilege classes on the router, one for configuring and viewing user accounts only and the second for configuring and viewing SNMP parameters only:

```
[edit]
system {
   login {
      class user-accounts {
         permissions [ configure admin admin-control ];
      }
      class network-mgmt {
         permissions [ configure snmp snmp-control ];
      }
   }
}
```

## *Denying or Allowing Individual Commands*

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the permissions statement. For information about CLI commands, see the *JUNOS CLI User Guide*.

**NOTE:** The all login class permission bits take precedence over extended regular expressions when a user with rollback permission issues the rollback command.

Expressions used to allow and deny commands for users on RADIUS/TACACS+ servers have been simplified. Instead of a single, long expression with multiple commands (allow-commands=cmd1 cmd2 cmdn) you can specify each command as a separate expression. This new syntax is valid for allow-configuration and deny-configuration, allow-command and deny-command, and user-permissions.

Users cannot issue the load override command when specifying an extended regular expression. Users can only issue the merge, replace, and patch configuration commands.

This section describes how to define a user's access privileges to individual operational and configuration mode commands. It contains the following topics:



### Specifying Operational Mode Commands

You can specify extended regular expressions with the allow-commands and deny-commands statements to define a user's access privileges to individual operational

commands. Doing so takes precedence over login class permission bits set for a user. You can include one deny-commands and one allow-commands statement in each login class.

To explicitly allow an individual operational mode command that would otherwise be denied, include the allow-commands statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
allow-commands "regular-expression";
```

To explicitly deny an individual operational mode command that would otherwise be allowed, include the deny-commands statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
deny-commands "regular-expression";
```

If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Regular expressions are not case-sensitive.

**NOTE:** Modifiers are not supported within the regular expression string to be matched. If a modifier is used, then nothing is matched.

For example, the deny command set protocols does not match anything whereas protocols matches *protocols*.

Use extended regular expressions to specify which operational mode commands are denied or allowed. You specify these regular expressions in the allow-commands and deny-commands statements at the [edit system login class] hierarchy level, or by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authentication server configuration. If regular expressions are received during TACACS+ or RADIUS authentication, they merge with any regular expressions configured on the local router. For information about TACACS+ or RADIUS authentication, see "Configuring System Authentication" on page 77.

Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2. Table 12 on page 66 lists common regular expression operators.

**Table 12: Common Regular Expression Operators to Allow or Deny Operational Mode Commands**

| Operator | Match |
|---|---|
| \| | One of two or more terms separated by the pipe (\|) symbol. Each term must be a complete standalone expression enclosed in parentheses ( ), with no spaces between the pipe and the adjacent parentheses. For example, (show system alarms)\|(show system software). |

**Table 12: Common Regular Expression Operators to Allow or Deny Operational Mode Commands** *(continued)*

| Operator | Match |
|---|---|
| ^ | At the beginning of an expression, used to denote where the command begins, and where there might be some ambiguity. |
| $ | Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces$" means that the user can issue the show interfaces command but cannot issue the show interfaces detail or show interfaces extensive command. |
| [ ] | Range of letters or digits. To separate the start and end of a range, use a hyphen ( - ). |
| ( ) | A group of commands, indicating a complete, standalone expression to be evaluated; the result is then evaluated as part of the overall expression. Parentheses must always be used in conjunction with pipe operators as explained above. |

If a regular expression contains a syntax error, it becomes invalid, and, although the user can log in, the permission granted or denied by the regular expression does not take effect. When regular expressions configured on TACACS+ or RADIUS servers merge with regular expressions configured on the router, if the final expression has a syntax error, the overall result is an invalid regular expression. If a regular expression does not contain any operators, all varieties of the command are allowed. For example, if the following statement is included in the configuration, the user can issue the commands show interfaces detail and show interfaces extensive in addition to showing an individual interface:

```
allow-commands "show interfaces";
```

### *Example 1: Defining Access Privileges to Individual Operational Mode Commands*

The following examples define user access privileges to individual operational mode commands.

If the following statement is included in the configuration and the user does not have the configure login class permission bit, the user can enter configuration mode:

```
[edit system login class class-name]
user@host# set allow-commands configure
```

If the following statement is included in the configuration and the user does not have the configure login class permission bit, the user can enter configuration exclusive mode:

```
[edit system login class class-name]
user@host# set allow-commands "configure exclusive"
```

**NOTE:** You cannot use runtime variables. In the following example, the runtime variable 1.2.3.4 cannot be used:

```
[edit system login class class-name]
user@host# set deny-commands "show bgp neighbor 1.2.3.4"
```

***Example 2: Configuring Access Privileges to Individual Operational Mode Commands***

Configure permissions for individual operational mode commands:

```
[edit]
system {
   login {
      # This login class has operator privileges and the additional ability to reboot the
      # router.
      class operator-and-boot {
         permissions [ clear network reset trace view ];
         allow-commands "request system reboot";
      }
      # This login class has operator privileges but can't use any commands beginning
      # with “set” .
      class operator-no-set {
         permissions [ clear network reset trace view ];
         deny-commands "^set";
      }
      # This login class has operator privileges and can install software but not view
      # BGP information, and can issue the show route command, without specifying
      # commands or arguments under it.
      class operator-and-install-but-no-bgp {
         permissions [ clear network reset trace view ];
         allow-commands "(request system software add)|(show route$)";
         deny-commands "show bgp";
      }
   }
}
```

## Specifying Configuration Mode Commands

You can specify extended regular expressions with the allow-configuration and deny-configuration attributes to define user access privileges to parts of the configuration hierarchy or individual configuration mode commands. Doing so overrides login class permission bits set for a user. You can also use wildcards to restrict access. When you define access privileges to parts of the configuration hierarchy or individual configuration mode commands, do the following:

- Specify the full paths in the extended regular expressions with the allow-configuration and deny-configuration attributes.
- Enclose parentheses around an extended regular expression that connects two or more expressions with the pipe | symbol. For example:

  [edit system login class *class-name*]

```
user@host# set deny-configuration "(system login class) | (system services)"
```

**NOTE:** Each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol. You cannot define access to keywords such as set, edit, or activate.

For more information about how to use wildcards, see Table 13 on page 69.

To explicitly allow an individual configuration mode command that would otherwise be denied, include the allow-configuration statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
allow-configuration "regular-expression";
```

To explicitly deny an individual configuration mode command that would otherwise be allowed, include the deny-configuration statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
deny-configuration “regular-expression";
```

If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Regular expressions are not case-sensitive.

You can include one deny-configuration and one allow-configuration statement in each login class.

Use extended regular expressions to specify which configuration mode commands are denied or allowed. You specify these regular expressions in the allow-configuration and deny-configuration statements at the [edit system login class] hierarchy level, or by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authentication server's configuration. If regular expressions are received during TACACS+ or RADIUS authentication, they merge with any regular expressions configured on the local router. For information about TACACS+ or RADIUS authentication, see “Configuring System Authentication” on page 77.

Command regular expressions implement the extended (modern) regular expressions, as defined in POSIX 1003.2. Table 13 on page 69 lists common regular expression operators.

**Table 13: Configuration Mode Commands—Common Regular Expression Operators**

| Operator | Match |
|---|---|
| \| | One of two or more terms separated by the pipe. Each term must be a complete standalone expression enclosed in parentheses ( ), with no spaces between the pipe and the adjacent parentheses. For example, (show system alarms)\|(show system software). |

**Table 13: Configuration Mode Commands—Common Regular Expression Operators** *(continued)*

| Operator | Match |
|---|---|
| ^ | At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity. |
| $ | Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces$" means that the user can issue the show interfaces command but cannot issue show interfaces detail or show interfaces extensive. |
| [ ] | Range of letters or digits. To separate the start and end of a range, use a hyphen ( - ). |
| ( ) | A group of commands, indicating a complete, standalone expression to be evaluated; the result is then evaluated as part of the overall expression. Parentheses must always be used in conjunction with pipe operators as explained above. |
| * | Zero or more terms. |
| + | One or more terms. |
| . | Any character except for a space " ". |

### *Example 3: Defining Access Privileges to Individual Configuration Mode Commands*

The following examples show how to configure access privileges to individual configuration mode commands.

If the following statement is included in the configuration and the user's login class permission bit is set to all, the user cannot configure telnet parameters:

```
[edit system login class class-name]
user@host# set deny-configuration "system services telnet"
```

If the following statement is included in the configuration and the user's login class permission bit is set to all, the user cannot issue login class commands within any login class whose name begins with "m":

```
[edit system login class class-name]
user@host# set deny-configuration "system login class m.*"
```

If the following statement is included in the configuration and the user's login class permission bit is set to all, the user cannot issue configuration mode commands at the login class or system services hierarchy levels:

```
[edit system login class class-name]
user@host# set deny-configuration "(system login class) | (system services)"
```

***Example 4: Configuring Access Privileges to Individual Configuration Mode Commands***

Configure permissions for individual configuration mode commands:

```
[edit]
system {
   login {
      # This login class has operator privileges and the additional ability to issue
      # commands at the system services hierarchy level.
      class only-system-services {
         permissions [ configure ];
         allow-configuration "system services";
      }
      # This login class has operator privileges but cannot issue any system
      # services commands.
      class all-except-system-services {
         permissions [ all ];
         deny-configuration "system services";
      }
   }
}
```

## *Configuring the Timeout Value for Idle Login Sessions*

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the router, even if that session is idle. To close idle sessions automatically, you configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes.

To define the timeout value for idle login sessions, include the idle-timeout statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
idle-timeout minutes;
```

Specify the number of minutes that a session can be idle before it is automatically closed.

If you have configured a timeout value, the CLI displays messages similar to the following when timing out an idle user. It starts displaying these messages 5 minutes before timing out the user.

```
user@host# Session will be closed in 5 minutes if there is no activity.
Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session
```

If you configure a timeout value, the session closes after the specified time has elapsed except if the user is running telnet or monitoring interfaces using the monitor interface or monitor traffic command.

### *Configuring Tips*

By default, the tip command is not enabled when a user logs in. To enable tips, include the login-tip statement at the [edit system login class *class-name*] hierarchy level:

```
[edit system login class class-name]
login-tip;
```

Adding this statement enables the tip command for the class specified, provided the user logs in using the CLI. For information about the tip command, see the *JUNOS CLI User Guide*.

## Configuring User Accounts

User accounts provide one way for users to access the router. (Users can access the router without accounts if you configured RADIUS or TACACS+ servers, as described in "Configuring User Authentication" on page 40.) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

To create user accounts, include the user statement at the [edit system login] hierarchy level:

```
[edit system login]
user username {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication {
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
```

For each user account, you can define the following:

- Username—(Optional) Name that identifies the user. It must be unique within the router. Do not include spaces, colons, or commas in the username. The username can be up to 64 characters long.
- User's full name—(Optional) If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and must be unique within the router. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.

- User's access privilege—(Required) One of the login classes you defined in the class statement at the [edit system login] hierarchy level, or one of the default classes listed in Table 13 on page 69.
- Authentication method or methods and passwords that the user can use to access the router—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that the JUNOS software encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the plain-text-password option, you are prompted to enter and confirm the password:

  ```
  [edit system login user router-name]
  user@host# set authentication plain-text-password
  New password: type password here
  Retype new password: retype password here
  ```

  The default requirements for plain-text passwords are:

  - The password must be between 6 and 128 characters long
    - You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
    - Valid passwords must contain at least one change of case or character class.

For each user account and for root logins, you can configure more than one public RSA or DSA key for user authentication. When a user logs in using a user account or as root, the configured public keys are referenced to determine whether the private key matches any of them. For an example of how to configure more than one public key for SSH authentication for a user account, see "Example: Configuring User Accounts" on page 74. For more information about how to configure root authentication, see "Configuring the Root Password" on page 53.

For SSH authentication, you can also copy the contents of an SSH keys file into the configuration. For information about how to specify filenames, see "Specifying Filenames and URLs" on page 36.

To load an SSH key file, use the load-key-file command. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys.

If you load the SSH keys file, the contents of the file are copied into the configuration immediately after you enter the load-key-file statement. To view the SSH keys entries, use the configuration mode show command. For example:

```
[edit system login user boojum]
user@host# set authentication load-key-file my-host:.ssh/identity.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
   ssh-rsa "1024 35 9727638204084251055468226757249864241630322
      207404962528390382038690141584534964170019610608358722961563
      475784918273603361276441874265946893207739108344813125957722
```

```
        625461667999278316123500438660915866283822489746732605661192
        181489539813862940327687806538169602027491641637359132693963
        44008443 boojum@juniper.net"; # SECRET-DATA
    }
```

An account for the user root is always present in the configuration. You configure the password for root using the root-authentication statement, as described in "Configuring the Root Password" on page 53.

JUNOS-FIPS and Common Criteria have special password requirements. FIPS and Common Criteria passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If JUNOS-FIPS is installed on the router, you cannot configure passwords unless they meet this standard. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

### *Example: Configuring User Accounts*

Create accounts for four router users, and create an account for the template user "remote." All users use one of the default system login classes. User alexander also has two DSA public keys configured for SSH authentication.

```
[edit]
system {
   login {
      user philip {
         full-name "Philip of Macedonia";
         uid 1001;
         class super-user;
         authentication {
            encrypted-password "$1$poPPeY";
         }
      }
      user alexander {
         full-name "Alexander the Great";
         uid 1002;
         class view;
         authentication {
            encrypted-password "$1$14c5.$sBopasdFFdssdfFFdsdfs0";
            ssh-dsa "8924 37 5678 5678@gaugamela.per";
            ssh-dsa "6273 94 9283@boojum.per";
         }
      }
      user darius {
         full-name "Darius King of Persia";
         uid 1003;
         class operator;
         authentication {
            ssh-rsa "1024 37 12341234@ecbatana.per";
         }
      }
      user anonymous {
         class unauthorized;
      }
```

```
        user remote {
            full-name "All remote users";
            uid 9999;
            class read-only;
        }
    }
}
```

## Limiting the Number of Login Attempts for SSH and Telnet Sessions

Beginning with JUNOS release 8.0, you can limit the number times a user can attempt to enter a password while logging in through SSH or Telnet. The connection is terminated if a user fails to log in after the number of attempts specified. You can also specify a delay, in seconds, before a user can try to enter a password after a failed attempt. In addition, you can specify the threshold for the number of failed attempts before the user experiences a delay in being able to enter a password again.

To specify the number of times a user can attempt to enter a password while logging in, include the retry-options statement at the [edit system login] hierarchy level:

```
[edit system login]
retry-options {
    tries-before-disconnect number;
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
}
password {
}
```

You can configure the following options.

- tries-before-disconnect—Number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 1 through 10, and the default is 10.
- backoff-threshold—Threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. Use the backoff-factor option to specify the length of the delay in seconds. The range is from 1 through 3, and the default is 2.
- backoff-factor—Length of time, in seconds, before a user can attempt to log in after a failed attempt. The delay increases by the value specified for each subsequent attempt after the threshold. The range is from 5 through 10, and the default is 5 seconds.
- minimum-time—Minimum length of time, in seconds, that a connection remains open while a user is attempting to enter a correct password. The range is from 20 through 60, and the default is 40.

### *Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions*

Limit the user four attempts when entering a password while logging in through SSH or Telnet. Set the backoff-threshold to 2, the back-off-factor to 5 seconds, and the

minimum-time to 40 seconds. The user experiences a delay of 5 seconds after the second attempt to enter a correct password fails. After each subsequent failed attempt, the delay increases by 5 seconds. After the fourth and final failed attempt to enter a correct password, the user experiences an additional 10-second delay, and the connection closes after a total of 40 seconds.

```
[edit]
system {
   login {
      retry-options {
         tries-before-disconnect 4;
         backoff-threshold 2;
         backoff-factor 5;
         minimum-time 40;
      }
      password {
      }
   }
}
```

## JUNOS-FIPS Crypto Officer and User Accounts

JUNOS-FIPS defines a restricted set of user roles. Unlike the JUNOS software, which allows a wide range of capabilities to users, FIPS 140-2 defines specific types of users (Crypto Officer, User, and Maintenance). Crypto Officers and FIPS Users perform all FIPS-related configuration tasks and issue all FIPS-related commands. Crypto Officer and FIPS User configurations must follow FIPS 140-2 guidelines. Typically, no user besides a Crypto Officer can perform FIPS-related tasks. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

### *Crypto Officer User Configuration*

JUNOS-FIPS offers finer control of user permissions than those mandated by FIPS 140-2. For FIPS 140-2 conformance, any JUNOS-FIPS user with the secret, security, and maintenance permission bits set is a Crypto Officer. In most cases, the super-user class should be reserved for a Crypto Officer. A FIPS User can be defined as any JUNOS-FIPS user that does not have the secret, security, and maintenance bits set.

### *FIPS User Configuration*

A Crypto Officer sets up FIPS Users. FIPS Users can be granted permissions normally reserved for a Crypto Officer; for example, permission to zeroize the system and individual AS-II FIPS PICs.

Chapter 7

# Configuring System Authentication

You can configure RADIUS or TACACS+ authentication, or both, as a method for authenticating users who attempt to access the router. This chapter includes information about how to configure RADIUS or TACACS+ authentication, create template accounts to authenticate multiple users, configure a local fallback method in the event the RADIUS or TACACS+ server is unavailable, and configure an authentication order.

This chapter provides information about how to configure user authentication on the router. This chapter includes the following topics:



## Configuring RADIUS Authentication

To use RADIUS authentication on the router, configure information about one or more RADIUS servers on the network by including one radius-server statement at the [edit system] hierarchy level for each RADIUS server:

```
[edit system]
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

*server-address* is the address of the RADIUS server.

You can specify a port on which to contact the RADIUS server. By default, port number 1812 is used (as specified in RFC 2865). You can also specify an accounting port to send accounting packets. The default is 1813 (as specified in RFC 2866).

You must specify a password in the secret *password* statement. If the password contains spaces, enclose it in quotation marks. The secret used by the local router must match that used by the server.

Optionally, you can specify the amount of time that the local router waits to receive a response from a RADIUS server (in the timeout statement) and the number of times that the router attempts to contact a RADIUS authentication server (in the retry statement). By default, the router waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds. By default, the router retries connecting to the server 3 times. You can configure this to be a value in the range from 1 through 10 times.

You can use the source-address statement to specify a logical address for individual or multiple RADIUS servers.

To configure multiple RADIUS servers, include multiple radius-server statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the user statement at the [edit system login] hierarchy level, as described in "Configuring Template Accounts for RADIUS and TACACS+ Authentication" on page 85.

You can also configure RADIUS authentication at the [edit access] and [edit access profile] hierarchy level. The JUNOS software uses the following search order to determine which set of servers are used for authentication:

[edit access profile *profile-name* radius-server *server-address*],
[edit access radius-server *server-address*],
[edit system radius-server *server-address*]

For more information, see "Configuring Access" on page 401.

## *Configuring Juniper Networks Vendor-Specific RADIUS Attributes*

The JUNOS software supports the configuration of Juniper Networks RADIUS vendor-specific attributes (VSAs). These VSAs are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 14 on page 79 lists the Juniper Networks VSAs you can configure.

**Table 14: Juniper Networks Vendor-Specific RADIUS Attributes**

| Name | Description | Type | Length | String |
|---|---|---|---|---|
| Juniper-Local-User-Name | Indicates the name of the user template used by this user when logging in to a device. This attribute is used only in Access-Accept packets. | 1 | ≥3 | One or more octets containing printable ASCII characters. |
| Juniper-Allow-Commands | Contains an extended regular expression that allows the user to run operational mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 2 | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 12 on page 66. |
| Juniper-Deny-Commands | Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 3 | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 12 on page 66. |
| Juniper-Allow-Configuration | Contains an extended regular expression that allows the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 4 | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 13 on page 69. |
| Juniper-Deny-Configuration | Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 5 | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 13 on page 69. |
| Juniper-Interactive-Command | Indicates the interactive command entered by the user. This attribute is used only in Accounting-Request packets. | 8 | ≥3 | One or more octets containing printable ASCII characters. |
| Juniper-Configuration-Change | Indicates the interactive command that results in a configuration (database) change. This attribute is used only in Accounting-Request packets. | 9 | ≥3 | One or more octets containing printable ASCII characters. |

**Table 14: Juniper Networks Vendor-Specific RADIUS Attributes** *(continued)*

| Name | Description | Type | Length | String |
|---|---|---|---|---|
| Juniper-User-Permissions | Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets.<br><br>**NOTE:** When the Juniper-User-Permissions attribute is configured to grant the JUNOS maintenance or all permissions on a RADIUS server, the UNIX wheel group membership is not automatically added to a user's list of group memberships . Some operations such as running the su root command from a local shell require wheel group membership permissions. However, when a user is configured locally with permissions maintenance or all, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account. For information about configuring user template accounts, see "Configuring Template Accounts for RADIUS and TACACS + Authentication" on page 85. | 10 | ≥3 | One or more octets containing printable ASCII characters.<br><br>The string is a list of permission flags separated by a space. The exact name of each flag must be specified in its entirety. See Table 11 on page 63. |

For more information about the VSAs, see RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

## *Configuring MS-CHAPv2 for Password-Change Support*

The JUNOS software enables you to configure Microsoft's implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router for password-change support. This feature provides users accessing a router the option of changing the password when the password expires, is reset, or is configured to be changed at next logon.

Before you configure MS-CHAPv2 for password-change support, ensure that you have done the following:

- Configured RADIUS server authentication parameters. For more information, see “Configuring RADIUS Authentication” on page 77.
- Set the first tried option in the authentication order to RADIUS server. For more information, see “Configuring the Authentication Order” on page 89.

To configure MS-CHAP-v2, include the following statements at the [edit system radius-options] hierarchy level:

```
[edit system radius-options]
password-protocol mschap-v2;
```

For an example configuration, see “Example: Configuring MS-CHAPv2 on the Router” on page 81.

### *Example: Configuring MS-CHAPv2 on the Router*

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
   authentication-order [ radius password ];
   radius-server {
      192.168.69.149 secret "$9$G-j.5Qz6tpBk.1hrlXxUjiq5Qn/C"; ## SECRET-DATA
   }
   radius-options {
      password-protocol mschap-v2;
   }
   login {
      user bob {
         class operator;
      }
   }
}
```

## Configuring TACACS+ Authentication

To use TACACS+ authentication on the router, configure information about one or more TACACS+ servers on the network by including the tacplus-server statement at the [edit system] hierarchy level:

```
[edit system]
tacplus-server server-address {
   port port-number;
   secret password;
   single-connection;
   timeout seconds;
}
```

*server-address* is the address of the TACACS+ server.

*port-number* is the TACACS+ server port number.

You must specify a secret (password) that the local router passes to the TACACS+ client by including the secret statement. If the password included spaces, enclose the password in quotation marks. The secret used by the local router must match that used by the server.

Optionally, you can specify the length of time that the local router waits to receive a response from a TACACS+ server by including the timeout statement. By default, the router waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can have the software maintain one open Transmission Control Protocol (TCP) connection to the server for multiple requests, rather than opening a connection for each connection attempt by including the single-connection statement.

**NOTE:** Early versions of the TACACS+ server do not support the single-connection option. If you specify this option and the server does not support it, the JUNOS software will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple tacplus-server statements.

On a TX Matrix platform, TACACS+ accounting should be configured only under the groups re0 and re1.

**NOTE:** Accounting should not be configured at the [edit system] hierarchy level; on a TX Matrix platform, control is done under the switch-card chassis only.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the user statement at the [edit system login] hierarchy level, as described in "Configuring Template Accounts for RADIUS and TACACS+ Authentication" on page 85.

### *Configuring Juniper Networks Vendor-Specific TACACS+ Attributes*

The TACACS attributes listed in Table 15 on page 83 are specific to Juniper Networks. They are specified in the TACACS+ server configuration file on a per-user basis. The JUNOS software retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user. You do not need to configure these attributes to run the JUNOS software with TACACS+.

To specify these attributes, include a service statement of the following form in the TACACS+ server configuration file:

```
service = junos-exec {
    local-user-name = <username-local-to-router>
    allow-commands = "<allow-commands-regex>"
    allow-configuration = "<allow-configuration-regex>"
    deny-commands = "<deny-commands-regex>"
    deny-configuration = "<deny-configuration-regex>"
}
```

This service statement can appear in a user or group statement.

**Table 15: Juniper Networks Vendor-Specific TACACS+ Attributes**

| Name | Description | Length | String |
|---|---|---|---|
| local-user-name | Indicates the name of the user template used by this user when logging in to a device. | ≥3 | One or more octets containing printable ASCII characters. |
| allow-commands | Contains an extended regular expression that allows the user to run operational mode commands in addition to those commands authorized by the user's login class permission bits. | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 12 on page 66. |
| allow-configuration | Contains an extended regular expression that allows the user to run configuration mode commands in addition to those commands authorized by the user's login class permission bits. | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 13 on page 69. |
| deny-commands | Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user's login class permission bits. | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 12 on page 66. |
| deny-configuration | Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user's login class permission bits. | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 13 on page 69. |

**Table 15: Juniper Networks Vendor-Specific TACACS+ Attributes** *(continued)*

| Name | Description | Length | String |
|---|---|---|---|
| user-permissions | Contains information the server uses to specify user permissions.<br><br>**NOTE:** When the user-permissions attribute is configured to grant the JUNOS maintenance or all permissions on a TACACS+ server, the UNIX wheel group membership is not automatically added to a user's list of group memberships . Some operations such as running the su root command from a local shell require wheel group membership permissions. However, when a user is configured locally with permissions maintenance or all, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account. For information about configuring user template accounts, see "Configuring Template Accounts for RADIUS and TACACS+ Authentication" on page 85. | ≥3 | One or more octets containing printable ASCII characters. See Table 11 on page 63. |

## Specifying a Source Address for RADIUS and TACACS+ Servers

You can specify which source address the JUNOS software uses when accessing your network to contact an external TACACS+ or RADIUS server for authentication. You can also specify which source address the JUNOS software uses when contacting a TACACS+ server for sending accounting information.

To specify a source address for a TACACS+ server for authentication, include the source-address statement at the [edit system tacplus-server *server-address*] hierarchy level:

```
[edit system tacplus-server server-address]
source-address source-address;
```

*source-address* is a valid IP address configured on one of the router interfaces.

To specify a source address for a TACACS+ server for system accounting, include the source-address statement at the [edit system accounting destination tacplus server *server-address*] hierarchy level:

```
[edit system accounting destination tacplus server server-address]
source-address source-address;
```

*source-address* is a valid IP address configured on one of the router interfaces.

To specify a source address for a RADIUS+ server, include the source-address statement at the [edit system radius-server *server-address*] hierarchy level:

```
[edit system radius-server server-address]
source-address source-address;
```

*source-address* is a valid IP address configured on one of the router interfaces.

**NOTE:** You can configure the JUNOS software to select a fixed address as the source address for locally generated IP packets. For more information, see "Configuring the Source Address for Locally Generated TCP/IP Packets" on page 143.

## Configuring the Same Authentication Service for Multiple TACACS+ Servers

To configure the same authentication service for multiple TACACS+ servers, include statements at the [edit system tacplus-server] and [edit system tacplus-options] hierarchy levels. For information about how to configure a TACACS+ server at the [edit system tacplus-server] hierarchy level, see "Configuring TACACS+ Authentication" on page 81.

To assign the same authentication service to multiple TACACS+ servers, include the service-name statement at the [edit system tacplus-options] hierarchy level:

```
[edit system tacplus-options]
service-name service-name;
```

*service-name* is the name of the authentication service. By default, the service name is set to junos-exec.

### *Example: Configuring Multiple TACACS+ Servers*

Configure the same authentication service for multiple TACACS+ servers:

```
[edit system]
tacplus-server {
    10.2.2.2 secret "$9$2dgoJGDiqP5ZG9A"; ## SECRET-DATA
    10.3.3.3 secret "$9$2dgoJGDiqP5ZG9A";## SECRET-DATA
}
tacplus-options {
    service-name bob;
}
```

## Configuring Template Accounts for RADIUS and TACACS+ Authentication

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

This section discusses the following topics:



### Using Remote Template Accounts

By default, the JUNOS software uses the remote template accounts when:

- The authenticated user does not exist locally on the router
- The authenticated user's record in the authentication server specifies local user, or the specified local user does not exist locally on the router

To configure the remote template account, include the user remote statement at the [edit system login] hierarchy level and specify the privileges you want to grant to remote users:

```
[edit system login]
user remote {
    full-name "All remote users";
    uid uid-value;
    class class-name;
}
```

To configure different access privileges for users who share the remote template account, include the allow-commands and deny-commands commands in the authentication server configuration file. For information about how to define access privileges on the authentication server, see "Configuring Juniper Networks Vendor-Specific RADIUS Attributes" on page 78 and "Configuring Juniper Networks Vendor-Specific TACACS+ Attributes" on page 82.

### Using Local User Template Accounts

You use local user template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template. These templates are defined locally on the router and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, the JUNOS software issues a request to the authentication server to authenticate the user's login name. If a user is authenticated, the server returns the local username to the JUNOS software, which then determines whether a local username is specified for that login name (local-username for TACACS+, Juniper-Local-User for RADIUS). If so, the JUNOS software selects the appropriate local user template locally configured on the router. If a local user template does not exist for the authenticated user, the router defaults to the remote template.

To configure different access privileges for users who share the local user template account, include the allow-commands and deny-commands commands in the authentication server configuration file. For information about how to configure access privileges on the authentication server, see "Configuring Juniper Networks

Vendor-Specific RADIUS Attributes” on page 78 and “Configuring Juniper Networks Vendor-Specific TACACS+ Attributes” on page 82.

To configure a local user template, include the user *local-username* statement at the [edit system login] hierarchy level and specify the privileges you want to grant to the local users to whom the template applies:

```
[edit system login]
user local-username {
   full-name "Local user account";
   uid uid-value;
   class class-name;
}
```

### Example: Using the Local User Template

In this example, you configure the sales and engineering local user templates:

```
[edit]
system {
   login {
      user sales {
         uid uid-value;
         class class-name;
      }
      user engineering {
         uid uid-value;
         class class-name;
      }
   }
}
```

Now you configure users on the TACACS+ authentication server:

```
user = simon {
   ...
   service = junos-exec {
      local-user-name = sales
      allow-commands = "configure"
      deny-commands = "shutdown"
   }
}
user = rob {
   ...
   service = junos-exec {
      local-user-name = sales
      allow-commands = "(request system) | (show rip neighbor)"
      deny-commands = "<^clear"
   }
}
user = harold {
   ...
   service = junos-exec {
      local-user-name = engineering
      allow-commands = "monitor | help | show | ping | traceroute"
```

```
        deny-commands = "configure"
    }
}
user = jim {
    ...
    service = junos-exec {
        local-user-name = engineering
        allow-commands = "show bgp neighbor"
        deny-commands = "telnet | ssh"
    }
}
```

When the login users Simon and Rob are authenticated, they use the sales local user template. When login users Harold and Jim are authenticated, they use the engineering local user template.

**NOTE:** Permission bits override allow and deny commands.

## Using Regular Expressions to Allow or Deny Access to Commands

Use regular expressions to specify which operational or configuration mode commands are allowed or denied when using a RADIUS or TACACS+ server for user authentication. You can specify the regular expressions using the appropriate Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authentication server configuration.

You can specify the allow, deny configuration or operational mode commands, or user-permissions in a single extended regular expression, enclosing the multiple commands in parentheses and separating them using the pipe symbol: allow-commands= (cmd1 | cmd2 | cmd*n*).

On a TACACS+ or RADIUS server, you can also use a simplified version for regular expressions, where you specify each command as a separate expression. The simplified version is valid for the Juniper-Allow-Commands, Juniper-Deny-Commands, Juniper-Allow-Configuration, Juniper-Deny-Configuration, and Juniper-User-Permissions vendor-specific attributes:

```
Juniper-Allow-Commands = "cmd1"
Juniper-Allow-Commands = "cmd2"
Juniper-Allow-Commands = "cmd n"
Juniper-Deny-Commands = "cmd1"
Juniper-Deny-Commands = "cmd2"
Juniper-Deny-Commands = "cmd n"
Juniper-Allow-Configuration = "cmd1"
Juniper-Allow-Configuration = "cmd2"
Juniper-Allow-Configuration = "cmd n"
Juniper-Deny-Configuration = "cmd1"
Juniper-Deny-Configuration = "cmd2"
Juniper-Deny-Configuration = "cmd n"
Juniper-User-Permissions = "cmd1"
Juniper-User-Permissions = "cmd2"
Juniper-User-Permissions = "cmd n"
```

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see "Configuring Juniper Networks Vendor-Specific RADIUS Attributes" on page 78 and "Configuring Juniper Networks Vendor-Specific TACACS+ Attributes" on page 82.

**NOTE:** When TACACS+ or RADIUS authentication is configured for a router, regular expressions configured on the RADIUS or TACACS+ server merge with any regular expressions configured on the local router at the [edit system login class] hierarchy level for the allow, deny, or permissions commands. If the final expression has a syntax error, the overall result is an invalid regular expression.

## Configuring the Authentication Order

Using the authentication-order statement, you can prioritize the order in which the JUNOS software tries the different authentication methods when verifying user access to a router.

To configure the authentication order, include the authentication-order statement at the [edit system] hierarchy level:

```
[edit system]
authentication-order [authentication-methods ];
```

Specify one or more of the following authentication methods in the preferred order, from first tried to last tried:

- radius—Verify the user using RADIUS authentication services
- tacplus—Verify the user using TACACS+ authentication services.
- password—Verify the user using the username and password configured locally by including the authentication statement at the [edit system login user] hierarchy level.

For each login attempt, the JUNOS software tries the configured authentication methods in order until the password is accepted. If the username and password are accepted, the login attempt succeeds and no other authentication methods are tried. The next method in the authentication order is consulted if the previous authentication method fails to respond OR if the method returns a reject response to the login attempt due to an incorrect username or password.

If none of the configured authentication methods accept the login credentials and if a reject response is received, the login attempt fails. If no response is received from any configured authentication method, the JUNOS software consults local password authentication as a last resort.

### *Using RADIUS or TACACS+ Authentication*

You can configure the JUNOS software to be both a RADIUS or TACACS+ authentication client.

If an authentication method included in the [authentication-order] statement is not available, or if the authentication is available but returns a reject response, the JUNOS software tries the next authentication method included in the authentication-order statement.

The RADIUS or TACACS+ server authentication might fail because of the following reasons:

- The authentication method is configured, but the corresponding authentication servers are not configured. For instance, the radius and tacplus authentication methods are included in the authentication-order statement, but the corresponding RADIUS or TACACS+ servers are not configured at the respective [edit system radius-server] and [edit system tacplus-server] hierarchy levels.
- The RADIUS or TACACS+ server does not respond within the timeout period configured at the [edit system radius-server] or [edit system tacplus-server] hierarchy levels.
- The RADIUS or TACACS+ server is not reachable due to a network problem.

The RADIUS or TACACS+ server authentication might return a reject response because of the following reasons:

- The user profiles of users accessing a router might not be configured on the RADIUS or TACACS+ server.
- The user enters incorrect logon credentials.

### *Using Local Password Authentication*

You can explicitly configure the password authentication method or use this method as a fallback mechanism when remote authentication servers fail. The password authentication method consults the local user profiles configured at the [edit system login] hierarchy level. Users can log in to a router using their local user name and password in the following scenarios:

- The password authentication method (password) is explicitly configured as one of the authentication methods in the [authentication-order *authentication-methods*] statement. In this case, the password authentication is consulted if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response due to an incorrect username or password.
- The password authentication method is not explicitly configured as one of the authentication methods in the [authentication-order *authentication-methods*] statement. In this case, the password authentication method is consulted only if all configured authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response due to an incorrect username or password.

### *Order of Authentication Attempts*

Table 16 on page 91 describes how the authentication-order statement at the [edit system] hierarchy level determines the procedure that the JUNOS software uses to authenticate users for access to a routing platform:

**Table 16: Order of Authentication Attempts**

| Syntax | Order of Authentication Attempts |
|---|---|
| authentication-order radius; | 1. Try configured RADIUS authentication servers.<br>2. If RADIUS server is available and authentication is accepted, grant access.<br>3. If RADIUS server is available but authentication is rejected, deny access.<br>4. If RADIUS servers are not available, try password authentication.<br>**NOTE:** If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order. |
| authentication-order [ radius password ]; | 1. Try configured RADIUS authentication servers.<br>2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order [ radius tacplus ]; | 1. Try configured RADIUS authentication servers.<br>2. If RADIUS server is available and authentication is accepted, grant access.<br>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.<br>4. If TACACS+ server is available and authentication is accepted, grant access.<br>5. If TACACS+ server is available but authentication is rejected, deny access.<br>6. If both RADIUS and TACACS+ servers are not available, try password authentication.<br>**NOTE:** If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order. |

**Table 16: Order of Authentication Attempts** *(continued)*

| Syntax | Order of Authentication Attempts |
|---|---|
| authentication-order [ radius tacplus password ]; | 1. Try configured RADIUS authentication servers.<br>2. If RADIUS server is available and authentication is accepted, grant access.<br>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.<br>4. If TACACS+ server is available and authentication is accepted, grant access.<br>5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order tacplus; | 1. Try configured TACACS+ authentication servers.<br>2. If TACACS+ server is available and authentication is accepted, grant access.<br>3. If TACACS+ server is available but authentication is rejected, deny access.<br>4. If TACACS+ servers are not available, try password authentication.<br>**NOTE:** If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order. |
| authentication-order [ tacplus password ]; | 1. Try configured TACACS+ authentication servers.<br>2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order [ tacplus radius ]; | 1. Try configured TACACS+ authentication servers.<br>2. If TACACS+ server is available and authentication is accepted, grant access.<br>3. If TACACS+ servers fail to respond or return a reject response try configured RADIUS servers.<br>4. If RADIUS server is available and authentication is accepted, grant access.<br>5. If RADIUS server is available but authentication is rejected, deny access.<br>6. If both TACACS+ and RADIUS servers are not available, try password authentication.<br>**NOTE:** If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order. |

**Table 16: Order of Authentication Attempts** *(continued)*

| Syntax | Order of Authentication Attempts |
|---|---|
| authentication-order [ tacplus radius password ]; | 1. Try configured TACACS+ authentication servers.<br>2. If TACACS+ server is available and authentication is accepted, grant access.<br>3. If TACACS+ servers fail to respond or return a reject response try configured RADIUS servers.<br>4. If RADIUS server is available and authentication is accepted, grant access.<br>5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order password; | 1. Try to authenticate the user, using the password configured at the [edit system login] hierarchy level.<br>2. If the authentication is accepted, grant access.<br>3. If the authentication is rejected, deny access. |

**NOTE:** If SSH public keys are configured, SSH user authentication first tries to perform public key authentication before using the authentication methods configured in the authentication-order statement. If you want SSH logins to use the authentication methods configured in the authentication-order statement without first trying to perform public key authentication, do not configure SSH public keys. For more information about loading SSH public keys, see "Importing Host Key Information from a File" on page 586.

### *Example: Removing an Order Set from the Authentication Order*

Delete the radius statement from the authentication order:

```
[edit system]
user@host# delete authentication-order radius
```

### *Example: Inserting an Order Set in the Authentication Order*

Insert the tacplus statement after the radius statement:

```
[edit system]
user@host# insert authentication-order tacplus after radius
```

## Examples: Configuring System Authentication

The following example allows logins only by the individual user Philip, and by users who have been authenticated by a remote RADIUS server. If a user logs in and is not

authenticated by the RADIUS server, the user is denied access to the router. However, if the RADIUS server is not available, the user's login name has a local password, and the user enters that password, the user is authenticated (using the password authentication method) and allowed access to the router. For more information about the password authentication method, see "Using Local Password Authentication" on page 90.

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the super-user class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the same privileges for the operator class.

```
[edit]
system {
   authentication-order radius;
   login {
      user philip {
         full-name "Philip";
         uid 1001;
         class super-user;
         user remote {
            full-name "All remote users";
            uid 9999;
            class operator;
         }
      }
   }
}
```

**NOTE:** For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see "Configuring Template Accounts for RADIUS and TACACS+ Authentication" on page 85.

Configuring a single remote user template account requires that all users without individual configuration entries share the same class and UID. When you are using RADIUS and telnet or RADIUS and SSH together, you can specify a different template user other than the remote user.

To configure an alternate template user, specify the user-name parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample JUNOS configuration:

```
[edit]
system {
   authentication-order radius;
   login {
      user philip {
         full-name "Philip";
         uid 1001;
         class super-user;
```

```
        }
        user operator {
            full-name "All operators";
            uid 9990;
            class operator;
        }
        user remote {
            full-name "All remote users";
            uid 9999;
            class read-only;
        }
    }
}
```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and username “operator”
- User Darius with password “redhead” and username “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser (super-user) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

## Recovering the Root Password

If you forget the root password for the router, you can use the password recovery procedure to reset the root password.

**NOTE:** You need console access to recover the root password.

To recover the root password:

1. Power off the router by pressing the power button on the front panel.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45 to DB-9 serial port adapter supplied with the router (see Figure 2 on page 96 and Figure 3 on page 96).
4. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device (see Figure 2 on page 96 and Figure 3 on page 96).
5. Connect the other end of the Ethernet rollover cable to the console port on the router (see Figure 2 on page 96 and Figure 3 on page 96).

**Figure 2: Connecting to the Console Port on the J2300 Services Router**

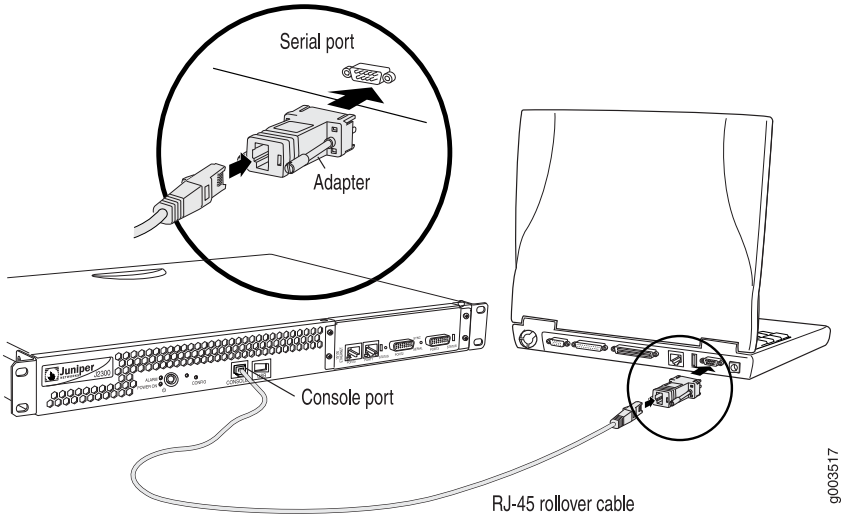
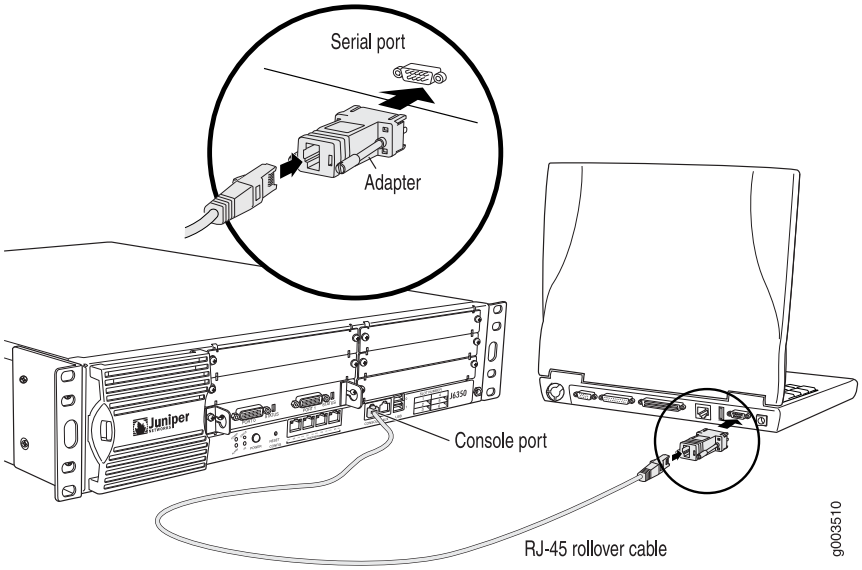



**Figure 3: Connecting to the Console Port on the J4350 or J6350 Services Router**




6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).
8. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None

- Stop bits: 1
- Flow control: None

9. Power on the router by pressing the power button on the front panel. Verify that the POWER LED on the front panel turns green.

   The terminal emulation screen on your management device displays the router's boot sequence.

10. When the following prompt appears, press the Spacebar to access the router's bootstrap loader command prompt:

```
Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 9 seconds...
```

11. At the following prompt, enter boot -s to start up the system in single-user mode.

```
ok boot -s
```

12. At the following prompt, enter recovery to start the root password recovery procedure.

```
Enter full pathname of shell or 'recovery' for root password recovery or
RETURN for /bin/sh: recovery
```

13. Enter configuration mode in the CLI.
14. Set the root password. For example:

```
user@host# set system root-authentication plain-text-password
```

    For more information about configuring the root password, see "Configuring the Root Password" on page 53

15. At the following prompt, enter the new root password. For example:

```
New password: juniper1
```

```
Retype new password:
```

16. At the second prompt, reenter the new root password.
17. If you are finished configuring the network, commit the configuration.

```
root@host# commit

commit complete
```

18. Exit configuration mode in the CLI.
19. Exit operational mode in the CLI.
20. At the prompt, enter y to reboot the router.

```
Reboot the system? [y/n] y
```

Chapter 8
# Configuring Time

This chapter discusses the following topics related to configuring time:



## Setting the Time Zone

The default local time zone on the router is UTC (Coordinated Universal Time, formerly known as Greenwich Mean Time, or GMT). To modify the local time zone, include the time-zone statement at the [edit system] hierarchy level:

```
[edit system]
time-zone (GMT<(+ | –)hour-offset> | time-zone);
```

You can use the GMT<(+ | –)*hour-offset*> option to set the time zone relative to UTC (GMT) time. By default, *hour-offset* is null (that is, the default is GMT without an offset). You can configure the offset to be a value in the range from –14 to +12.

You can also specify *time-zone* as a string such as PDT (Pacific Daylight Time) or WET (Western European Time), or specify the continent and major city.

For the time zone change to take effect for all processes running on the router, you must reboot the router.

### *Examples: Setting the Time Zone*

Set the time zone relative to UTC (GMT):

```
[edit]
user@host# set system time-zone GMT+2
```

Set the time zone for Pacific Daylight Time:

```
[edit]
user@host# set system time-zone PDT
[edit]
user@host# show
system {
    time-zone PDT;
```

```
}
```

Set the time zone for New York:

```
[edit]
user@host# set system time-zone America/New_York
[edit]
user@host# show
system {
    time-zone America/New_York;
}
```

For information about what time zones are available, see time-zone.

## Configuring the Network Time Protocol

NTP provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse network. NTP uses a returnable-time design in which a distributed subnet of time servers operating in a self-organizing, hierarchical primary-secondary configuration synchronizes local clocks within the subnet and to national time standards by means of wire or radio. The servers also can redistribute reference time using local routing algorithms and time daemons.

NTP is defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

For Common Criteria compliance, configure NTP to provide accurate timestamps for system log messages. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

**NOTE:** NTP does not support VPN routing and forwarding (VRF) requests. The router cannot process these requests properly because NTP uses the inet.0 route table for route resolution to the requestor and thus cannot propagate routes using the *routing-instance-name*.inet.0 VRF table for the VPN.

To configure NTP on the router, include the ntp statement at the [edit system] hierarchy level:

```
[edit system]
ntp {
    authentication-key number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    server address <key key-number> <version value> <prefer>;
    source-address source-address;
    trusted-key [ key-numbers ];
}
```

When configuring NTP, you do not actively configure time servers. Rather, all clients also are servers. An NTP server is not believed unless it, in turn, is synchronized to another NTP server—which itself must be synchronized to something upstream, eventually terminating in a high-precision clock.

By default, if the time difference between the local router clock and the NTP server clock is more than 128 milliseconds, the clocks are slowly stepped into synchronization. However, if the difference is more than 1000 seconds, the clocks are not synchronized. On the local router, you set the date and time using the set date command. To set the time automatically, use the boot-server statement at the [edit system ntp] hierarchy level, specifying the address of an NTP server.

This section includes the following information:



## Configuring the NTP Boot Server

When you boot the router, it issues an ntpdate request, which polls a network server to determine the local date and time. You need to configure a server that the router uses to determine the time when the router boots. Otherwise, NTP will not be able to synchronize to a time server if the server's time appears to be very far off of the local router's time.

To configure the NTP boot server, include the boot-server statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
boot-server address;
```

Specify the address of the network server. You must specify an address, not a hostname.

## Specifying a Source Address for an NTP Server

For IP version 4 (IPv4), you can specify that if the NTP server configured at the [edit system ntp] hierarchy level is contacted on one of the loopback interface addresses, the reply always uses a specific source address. This is useful for controlling which source address NTP will use to access your network when it is either responding to an NTP client request from your network or when it itself is sending NTP requests to your network.

To configure the specific source address that the reply will always use, and the source address that requests initiated by NTP server will use, include the source-address statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
source-address source-address;
```

*source-address* is a valid IP address configured on one of the router interfaces.

## Configuring the NTP Time Server and Time Services

When configuring NTP, you can specify which system on the network is the authoritative time source, or time server, and how time is synchronized between systems on the network. To do this, you configure the router to operate in one of the following modes:

- Client mode—In this mode, the local router can be synchronized with the remote system, but the remote system can never be synchronized with the local router.
- Symmetric active mode—In this mode, the local router and the remote system can synchronize with each other. You use this mode in a network in which either the local router or the remote system might be a better source of time.

**NOTE:** Symmetric active mode can be initiated by either the local or the remote system. Only one system needs to be configured to do so. This means that the local system can synchronize with any system that offers symmetric active mode without any configuration whatsoever. However, we strongly encourage you to configure authentication to ensure that the local system synchronizes only with known time servers.

- Broadcast mode—In this mode, the local router sends periodic broadcast messages to a client population at the specified broadcast or multicast *address*. Normally, you include this statement only when the local router is operating as a transmitter.
- Server mode—In this mode, the local router operates as an NTP server.

**NOTE:** In NTP server mode, the JUNOS software does not support authentication.

The following sections describe how to configure these modes of operation:


- Configuring the Router to Operate in Client Mode on page 102
- Configuring the Router to Operate in Symmetric Active Mode on page 103
- Configuring the Router to Operate in Broadcast Mode on page 104
- Configuring the Router to Operate in Server Mode on page 104


### Configuring the Router to Operate in Client Mode

To configure the local router to operate in client mode, include the server statement and other optional statements at the [edit system ntp] hierarchy level:

```
[edit system ntp]
```

```
server address <key key-number> <version value> <prefer>;
authentication-key key-number type type value password;
boot-server address;
trusted-key [ key-numbers ];
```

Specify the address of the system acting as the time server. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the time server, include the key option. The key corresponds to the key number you specify in the authentication-key statement, as described in "Configuring NTP Authentication Keys" on page 105.

By default, the router sends NTP version 4 packets to the time server. To set the NTP version level to 1, 2, or 3 include the version option.

If you configure more than one time server, you can mark one server preferred by including the prefer option.

For information about how to configure trusted keys, see "Configuring NTP Authentication Keys" on page 105. For information about how to configure an NTP boot server, see "Configuring the NTP Boot Server" on page 101. For information about how to configure the router to operate in server mode, see "Configuring the Router to Operate in Server Mode" on page 104.

#### *Example: Configuring Client Mode*

Configure the router to operate in client mode:

```
[edit system ntp]
authentication-key 1 type md5 value "$9$EgfcrvX7VY4ZEcwgoHjkP5Q3CuREyv87";
boot-server 10.1.1.1;
server 10.1.1.1 key 1 prefer;
trusted-key 1;
```

### Configuring the Router to Operate in Symmetric Active Mode

To configure the local router to operate in symmetric active mode, include the peer statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
peer address <key key-number> <version value> <prefer>;
```

Specify the address of the remote system. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the remote system, include the key option. The key corresponds to the key number you specify in the authentication-key statement, as described in "Configuring NTP Authentication Keys" on page 105.

By default, the router sends NTP version 4 packets to the remote system. To set the NTP version level to 1, 2 or 3, include the version option.

If you configure more than one remote system, you can mark one system preferred by including the prefer option:

```
peer address <key key-number> <version value> prefer;
```

### Configuring the Router to Operate in Broadcast Mode

To configure the local router to operate in broadcast mode, include the broadcast statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
broadcast address <key key-number> <version value> <ttl value>;
```

Specify the broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be 224.0.1.1.

To include an authentication key in all messages sent to the remote system, include the key option. The key corresponds to the key number you specify in the authentication-key statement, as described in “Configuring NTP Authentication Keys” on page 105.

By default, the router sends NTP version 4 packets to the remote system. To set the NTP version level to 1, 2, or 3, include the version option.

### Configuring the Router to Operate in Server Mode

In server mode, the router acts as an NTP server for clients when the clients are configured appropriately. The only prerequisite for “ server mode” is that the router must be receiving time from another NTP peer or server. No other configuration is necessary on the router.

To configure the local router to operate as an NTP server, include the following statements at the [edit system ntp] hierarchy level:

```
[edit system ntp]
authentication-key key-number type type value password;
server address <key key-number> <version value> <prefer>;
trusted-key [ key-numbers ];
```

Specify the address of the system acting as the time server. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the time server, include the key option. The key corresponds to the key number you specify in the authentication-key statement, as described in “Configuring NTP Authentication Keys” on page 105.

By default, the router sends NTP version 4 packets to the time server. To set the NTP version level to 1,or 2, or 3, include the version option.

If you configure more than one time server, you can mark one server preferred by including the prefer option.

For information about how to configure trusted keys, see “Configuring NTP Authentication Keys” on page 105. For information about how to configure the router to operate in client mode, see “Configuring the Router to Operate in Client Mode” on page 102.

#### *Example: Configuring Server Mode*

Configure the router to operate in server mode:

```
[edit system ntp]
authentication-key 1 type md5 value "$9$txERuBEreWx-wtuLNdboaUjH.T3AtOESe";
server 172.17.27.46 prefer;
trusted-key 1;
```

## *Configuring NTP Authentication Keys*

Time synchronization can be authenticated to ensure that the local router obtains its time services only from known sources. By default, network time synchronization is unauthenticated. The system will synchronize to whatever system appears to have the most accurate time. We strongly encourage you to configure authentication of network time services.

To authenticate other time servers, include the trusted-key statement at the [edit system ntp] hierarchy level. Only time servers transmitting network time packets that contain one of the specified key numbers and whose key matches the value configured for that key number are eligible to be synchronized to. Other systems can synchronize to the local router without being authenticated.

```
[edit system ntp]
trusted-key [ key-numbers ];
```

Each key can be any 32-bit unsigned integer except 0. Include the key option in the peer, server, or broadcast statements to transmit the specified authentication key when transmitting packets. The key is necessary if the remote system has authentication enabled so that it can synchronize to the local system.

To define the authentication keys, include the authentication-key statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
authentication-key key-number type type value password;
```

*number* is the key number, *type* is the authentication type (only Message Digest 5 [MD5] is supported), and *password* is the password for this key. The key number, type, and password must match on all systems using that particular key for authentication.

## *Configuring the Router to Listen for Broadcast Messages*

When you are using NTP, you can configure the local router to listen for broadcast messages on the local network to discover other servers on the same subnet by including the broadcast-client statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
broadcast-client;
```

When the router hears a broadcast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *broadcast client* mode, in which it listens for, and synchronizes to, succeeding broadcast messages.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

### *Configuring the Router to Listen for Multicast Messages*

When you are using NTP, you can configure the local router to listen for multicast messages on the local network to discover other servers on the same subnet by including the multicast-client statement at the [edit system ntp] hierarchy level:

```
[edit system ntp]
multicast-client <address>;
```

When the router hears a multicast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *multicast client* mode, in which it listens for, and synchronizes to, succeeding multicast messages.

You can specify one or more IP addresses. (You must specify an address, not a hostname.) If you do, the route joins those multicast groups. If you do not specify any addresses, the software uses 224.0.1.1.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

## Setting a Custom Time Zone

You can update the time zone database information on routers running the JUNOS software, independently of the JUNOS operating system. This feature simplifies time zone management in JUNOS systems by allowing for future unforeseen time zone database adjustments. You can configure your router to use a custom time zone database file that you create to meet your requirements by editing an existing time zone database file.

### *Usage Guidelines for Setting a Custom Time Zone*

To use a custom time zone, follow these steps:

1. Download a time zones archive (from a known or designated source) to the router. Compile the time zone archive using the *zic* time zone compiler, which generates *tz* files.
2. Using the CLI, configure the router to enable the use of the generated tz files as follows:

   ```
   [edit]
   ```

```
user@host# set system use-imported-time-zones
```

3. Display the imported time zones (saved in the directory /var/db/zoneinfo/):

```
[edit]
user@host# set system time-zone ?
```

If you do not configure for using imported time zones, the JUNOS default time zones are shown (saved in the directory /usr/share/zoneinfo/).

### How to Import and Install Time Zone Files

To import and install time zone files, follow these steps:

1. Download the time zone files archive and untar them to a temporary directory such as /var/tmp:

```
# mkdir -p /var/tmp/tz && cd /var/tmp/tz && rm *
# wget 'ftp://elsie.nci.nih.gov/pub/tzdata*.tar.gz'
# tar xvzf tzdata*.gz
africa
antarctica
asia
australasia
europe
northamerica
southamerica
pacificnew
etcetera
factory
backward
systemv
solar87
solar88
solar89
iso3166.tab
zone.tab
leapseconds
yearistype.sh
```

**NOTE:** If needed, you can edit the above untarred files to create or modify time zones.

2. Select the names of time zone files to compile and feed them to the following script.
For example, to generate northamerica and asia tz files:

```
# /usr/libexec/ui/compile-tz northamerica asia
```

3. Enable the use of the generated tz files using the CLI:

```
[edit]
# set system use-imported-time-zones
```

```
[edit]
# set system time-zone ?
```

This should show the newly generated tz files in /var/db/zoneinfo/.

4. Set the time zone and commit:

```
[edit]
# set system time-zone <your-time-zone>
# commit
```

5. Verify that the time zone change has taken effect:

```
[edit]
# run show system uptime
```

Chapter 9

# Configuring System Log Messages

The JUNOS software generates system log messages (also called *syslog messages*) to record events that occur on the routing platform, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a peer process
- Emergency or critical conditions, such as routing platform power-down due to excessive temperature

Each system log message identifies the JUNOS software process that generated the message and briefly describes the operation or error that occurred. This chapter explains how to configure system logging. For detailed information about specific system log messages, see the *JUNOS System Log Messages Reference*.

**NOTE:** The configuration hierarchy in this chapter applies to JUNOS software processes and libraries, not to the services on a Physical Interface Card (PIC) such as the Adaptive Services PIC. For information about configuring system logging for PIC services, see the *JUNOS Services Interfaces Configuration Guide*.

This chapter discusses the following topics:



## System Logging Configuration Statements

To configure the routing platform to log system messages, include the **syslog** statement at the [edit system] hierarchy level:

```
[edit system]
syslog {
    archive {
        files number;
        size size;
```

```
        (world-readable | no-world-readable);
    }
    console {
        facility severity;
    }
    file filename {
        facility severity;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
        archive {
            archive-sites {
                site-name;
            }
            files number;
            size size;
            start-time date.time;
            transfer-interval interval;
            (world-readable | no-world-readable);
        }
    }
    host (hostname | other-routing-engine | scc-master) {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string
        match "regular-expression";
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

## Minimum and Default System Logging Configuration

For information about the minimum and default system log settings on routing platforms that run the JUNOS software, see the following sections:

- Minimum System Logging Configuration on page 110
- Default System Log Settings on page 111

### *Minimum System Logging Configuration*

To record or view system log messages, you must include the **syslog** statement at the [edit system] hierarchy level. Specify at least one destination for the messages, as described in Table 17 on page 111. For more information about the configuration statements, see "Configuring System Logging for a Single-Chassis System" on page 113.

**Table 17: Minimum Configuration Statements for System Logging**

| Destination | Minimum Configuration Statements |
|---|---|
| File | [edit system syslog]<br>file *filename* {<br>  *facility severity*;<br>} |
| Terminal session of one, several, or all users | [edit system syslog]<br>user (*username* \| *) {<br>  *facility severity*;<br>} |
| Routing platform console | [edit system syslog]<br>console {<br>  *facility severity*;<br>} |
| Remote machine or the other Routing Engine on the routing platform | [edit system syslog]<br>host (*hostname* \| other-routing-engine) {<br>  *facility severity*;<br>} |

## *Default System Log Settings*

Table 18 on page 111 summarizes the default system log settings that apply to all platforms that run the JUNOS software, and specifies which statement to include in the configuration to override the default value.

**Table 18: Default System Logging Settings**

| Setting | Default | Overriding Statement | Instructions |
|---|---|---|---|
| Alternative facility for message forwarded to a remote machine | For change-log: local6<br>For conflict-log: local5<br>For dfc: local1<br>For firewall: local3<br>For interactive-commands: local7<br>For pfe: local4 | [edit system syslog]<br>host *hostname* {<br>  facility-override *facility*;<br>} | "Changing the Alternative Facility Name for Remote Messages" on page 120 |
| Format of messages logged to a file | Standard JUNOS format, based on UNIX format | [edit system syslog]<br>file *filename* {<br>  structured-data;<br>} | "Logging Messages in Structured-Data Format" on page 117 |

**Table 18: Default System Logging Settings** *(continued)*

| Setting | Default | Overriding Statement | Instructions |
|---|---|---|---|
| Maximum number of files in the archived set | 10 | [edit system syslog]<br>archive {<br>  files *number*;<br>}<br>file *filename* {<br>  archive {<br>  files *number*;<br>  }<br>} | "Specifying Log File Size, Number, and Archiving Properties" on page 123 |
| Maximum size of log file | J-series: 128 kilobytes (KB)<br><br>M-series, MX-series, and T-series: 1 megabyte (MB)<br><br>TX Matrix: 10 MB | [edit system syslog]<br>archive {<br>  size *size*;<br>}<br>file *filename* {<br>  archive {<br>  size *size*;<br>  }<br>} | "Specifying Log File Size, Number, and Archiving Properties" on page 123 |
| Timestamp format | Month, date, hour, minute, second<br><br>For example: Aug 21 12:36:30 | [edit system syslog]<br>time-format *format*; | "Including the Year or Millisecond in Timestamps" on page 127 |
| Users who can read log files | root user and users with the JUNOS maintenance permission | [edit system syslog]<br>archive {<br>  world-readable;<br>}<br>file *filename* {<br>  archive {<br>  world-readable;<br>  }<br>} | "Specifying Log File Size, Number, and Archiving Properties" on page 123 |

In addition, the following messages are generated by default on specific platforms. To view either type of message, you must configure at least one destination for messages as described in "Minimum System Logging Configuration" on page 110.

- On J-series platforms, a message is logged when a process running in the kernel consumes 500 or more consecutive milliseconds of CPU time.

  To log the message on an M-series, MX-series, or T-series platform, include the kernel info statement at the appropriate hierarchy level:

  ```
  [edit system syslog]
  (console | file filename | host destination | user username) {
    kernel info;
  }
  ```

- The master Routing Engine on each T640 routing node in a routing matrix forwards to the master Routing Engine on the TX Matrix platform all messages with a severity of info and higher. This is equivalent to the following configuration statement included on the TX Matrix platform:

```
[edit system syslog]
host scc-master {
    any info;
}
```

## Configuring System Logging for a Single-Chassis System

The JUNOS system logging utility is similar to the UNIX syslogd utility. This section describes how to configure system logging for a single-chassis system that runs the JUNOS software.

System logging configuration for the JUNOS-FIPS software and for Juniper Networks routing platforms in a Common Criteria environment is the same as for the JUNOS software. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

For information about configuring system logging for a routing matrix, see "Configuring System Logging for a Routing Matrix" on page 132.

Each system log message belongs to a *facility*, which groups together related messages. Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects routing platform functions. You always specify the facility and severity of the messages to include in the log. For more information, see

You direct messages to one or more destinations by including the appropriate statement at the [edit system syslog] hierarchy level:

- To a named file in a local file system, by including the file statement. See "Directing Messages to a Log File" on page 116.
- To the terminal session of one or more specific users (or all users) when they are logged in to the routing platform, by including the user statement. See "Directing Messages to a User Terminal" on page 118.
- To the routing platform console, by including the console statement. See "Directing Messages to the Console" on page 118.
- To a remote machine that is running the syslogd utility or to the other Routing Engine on the routing platform, by including the host statement. See "Directing Messages to a Remote Machine or the Other Routing Engine" on page 118.

By default, messages are logged in a standard format, which is based on a UNIX system log format; for detailed information about message formatting, see the *JUNOS System Log Messages Reference*. You can alter the content and format of logged messages in the following ways:

- In JUNOS Release 8.3 and later, you can log messages to a file in structured-data format instead of the standard JUNOS format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from the message. For more information, see "Logging Messages in Structured-Data Format" on page 117.
- A message's facility and severity level are together referred to as its *priority*. By default, the standard JUNOS format for messages does not include priority information. is not included in system log messages. (Structured-data format includes a priority code by default.) To include priority information in standard-format messages directed to a file or a remote destination, include the explicit-priority statement. For more information, see "Including Priority Information in System Log Messages" on page 125.
- By default, the standard JUNOS format for messages specifies the month, date, hour, minute, and second when the message was logged. You can modify the timestamp on standard-format system log messages to include the year, the millisecond, or both. (Structured-data format specifies the year and millisecond by default.) For more information, see "Including the Year or Millisecond in Timestamps" on page 127.
- When directing messages to a remote machine, you can specify the IP address that is reported in messages as their source. You can also configure features that make it easier to separate messages generated by the JUNOS software or messages generated on particular routing platforms. For more information, see "Directing Messages to a Remote Machine or the Other Routing Engine" on page 118.
- The predefined facilities group together related messages, but you can also use regular expressions to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination. For more information, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 128.

For detailed information about configuring system logging, see the following sections:

### *Specifying the Facility and Severity of Messages to Include in the Log*

Each system log message belongs to a *facility*, which is a group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects routing platform functions.

When you configure logging for a facility and destination, you specify a severity level for each facility. Messages from the facility that are rated at that level or higher are logged to the destination:

```
[edit system syslog]
(console | file filename | host destination | user username) {
    facility severity;
}
```

(For information about the destinations, see "Directing Messages to a Log File" on page 116, "Directing Messages to a User Terminal" on page 118, "Directing Messages to the Console" on page 118, and "Directing Messages to a Remote Machine or the Other Routing Engine" on page 118.)

To log the messages belonging to more than one facility to a particular destination, specify each facility name as a separate statement within the set of statements for the destination.

Table 19 on page 115 lists the JUNOS system logging facilities that you can specify in configuration statements at the [edit system syslog] hierarchy level.

**Table 19: JUNOS System Logging Facilities**

| Facility | Type of Event or Error |
|---|---|
| any | All (messages from all facilities) |
| authorization | Authentication and authorization attempts |
| change-log | Changes to the JUNOS configuration |
| conflict-log | Specified configuration is invalid on the routing platform type |
| daemon | Actions performed or errors encountered by system processes |
| dfc | Events related to dynamic flow capture |
| firewall | Packet filtering actions performed by a firewall filter |
| ftp | Actions performed or errors encountered by the FTP process |
| interactive-commands | Commands issued at the JUNOS command-line interface (CLI) prompt or by a client application such as a JUNOScript or NETCONF client |
| kernel | Actions performed or errors encountered by the JUNOS kernel |
| pfe | Actions performed or errors encountered by the Packet Forwarding Engine |

**Table 19: JUNOS System Logging Facilities** *(continued)*

| Facility | Type of Event or Error |
|---|---|
| user | Actions performed or errors encountered by user-space processes |

Table 20 on page 116 lists the severity levels that you can specify in configuration statements at the [edit system syslog] hierarchy level. The levels from emergency through info are in order from highest severity (greatest effect on functioning) to lowest.

Unlike the other severity levels, the none level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see "Disabling Logging of a Facility" on page 130.

**Table 20: System Log Message Severity Levels**

| Severity Level | Description |
|---|---|
| any | Includes all severity levels |
| none | Disables logging of the associated facility to a destination |
| emergency | System panic or other condition that causes the routing platform to stop functioning |
| alert | Conditions that require immediate correction, such as a corrupted system database |
| critical | Critical conditions, such as hard errors |
| error | Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels |
| warning | Conditions that warrant monitoring |
| notice | Conditions that are not errors but might warrant special handling |
| info | Events or nonerror conditions of interest |

## *Directing Messages to a Log File*

To direct system log messages to a file in the /var/log directory of the local Routing Engine, include the file statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
file filename {
    facility severity;
    explicit-priority;
    match "regular-expression";
    structured-data {
        brief;
```

```
    }
    archive {
      files number;
      size size;
      (world-readable | no-world-readable);
    }
  }
```

For the list of facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 115.

To prevent log files from growing too large, the JUNOS system logging utility by default writes messages to a sequence of files of a defined size. By including the archive statement, you can configure the number of files, their maximum size, and who can read them, for either all log files or a certain log file. For more information, see "Specifying Log File Size, Number, and Archiving Properties" on page 123.

For information about the following statements, see the indicated sections:

- explicit-priority—See "Including Priority Information in System Log Messages" on page 125
- match—See "Using Regular Expressions to Refine the Set of Logged Messages" on page 128
- structured-data—See "Logging Messages in Structured-Data Format" on page 117

## Logging Messages in Structured-Data Format

In JUNOS Release 8.3 and later, you can log messages to a file in structured-data format instead of the standard JUNOS format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from a message.

The structured-data format complies with Internet draft draft-ietf-syslog-protocol-23.txt, *The syslog Protocol*, which at the time of this writing is accessible at http://www.ietf.org/internet-drafts/draft-ietf-syslog-protocol-23.txt. The draft establishes a standard message format regardless of the source or transport protocol for logged messages.

To output messages to a file in structured-data format, include the structured-data statement at the [edit system syslog file *filename*] hierarchy level:

```
[edit system syslog file filename]
facility severity;
structured-data {
  brief;
}
```

The optional brief statement suppresses the English-language text that appears by default at the end of a message to describe the error or event. For information about the fields in a structured-data format message, see the *JUNOS System Log Messages Reference*.

The structured format is used for all messages logged to the file that are generated by a JUNOS process or software library.

**NOTE:** If you include either or both of the explicit-priority and time-format statements along with the structured-data statement, they are ignored. These statements apply to the standard JUNOS system log format, not to structured-data format.

### *Directing Messages to a User Terminal*

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged in to the local Routing Engine, include the user statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
user (username | *) {
    facility severity;
    match "regular-expression";
}
```

Specify one or more JUNOS usernames, separating multiple values with spaces, or use the asterisk (*) to indicate all users who are logged in to the local Routing Engine.

For the list of logging facilities and severity levels, see “Specifying the Facility and Severity of Messages to Include in the Log” on page 115. For information about the match statement, see “Using Regular Expressions to Refine the Set of Logged Messages” on page 128.

### *Directing Messages to the Console*

To direct system log messages to the console of the local Routing Engine, include the console statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
console {
    facility severity;
}
```

For the list of logging facilities and severity levels, see “Specifying the Facility and Severity of Messages to Include in the Log” on page 115.

### *Directing Messages to a Remote Machine or the Other Routing Engine*

To direct system log messages to a remote machine or to the other Routing Engine on the routing platform, include the host statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
```

```
    log-prefix string;
    match "regular-expression";
}
source-address source-address;
```

To direct system log messages to a remote machine, include the host *hostname* statement to specify the remote machine's IP version 4 (IPv4) address, IP version 6 (IPv6) address, or fully qualified hostname. The remote machine must be running the standard syslogd utility. We do not recommend directing messages to another Juniper Networks routing platform. In each system log message directed to the remote machine, the hostname of the local Routing Engine appears after the timestamp to indicate that it is the source for the message.

To direct system log messages to the other Routing Engine on a routing platform with two Routing Engines installed and operational, include the host other-routing-engine statement. The statement is not automatically reciprocal, so you must include it in each Routing Engine's configuration if you want them to direct messages to each other. In each message directed to the other Routing Engine, the string re0 or re1 appears after the timestamp to indicate the source for the message.

For the list of logging facilities and severity levels to configure under the host statement, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 115.

To record facility and severity level information in each message, include the explicit-priority statement. For more information, see "Including Priority Information in System Log Messages" on page 125.

For information about the match statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 128.

When directing messages to remote machines, you can include the source-address statement to specify the IP address of the routing platform that is reported in the messages as their source. In each host statement, you can also include the facility-override statement to assign an alternative facility and the log-prefix statement to add a string to each message. For more information, see the following sections:

- Specifying an Alternative Source Address for System Log Messages on page 119
- Changing the Alternative Facility Name for Remote Messages on page 120
- Adding a Text String to System Log Messages on page 122

### Specifying an Alternative Source Address for System Log Messages

To specify the routing platform that is reported in system log messages as their source when they are directed to a remote machine, include the source-address statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
source-address source-address;
```

*source-address* is a valid IPv4 or IPv6 address configured on one of the routing platform interfaces. The address is reported in the messages directed to all remote machines

specified in host *hostname* statements at the [edit system syslog] hierarchy level, but not in messages directed to the other Routing Engine.

### Changing the Alternative Facility Name for Remote Messages

Some facilities assigned to messages logged on the local routing platform have the JUNOS software-specific names (see Table 19 on page 115). In the recommended configuration, a remote machine designated at the [edit system syslog host *hostname*] hierarchy level is not a Juniper Networks routing platform, so its syslogd utility cannot interpret the JUNOS software-specific names. To enable the standard syslogd utility to handle messages from these facilities when messages are directed to a remote machine, a standard local*X* facility name is used instead of the JUNOS software-specific facility name.

Table 21 on page 120 lists the default alternative facility name next to the JUNOS software-specific facility name it is used for. For facilities that are not listed, the default alternative name is the same as the local facility names.

**Table 21: Default Facilities for Messages Directed to a Remote Destination**

| JUNOS Software-Specific Local Facility | Default Facility When Directed to Remote Destination |
|---|---|
| change-log | local6 |
| conflict-log | local5 |
| dfc | local1 |
| firewall | local3 |
| interactive-commands | local7 |
| pfe | local4 |

The syslogd utility on a remote machine handles all messages that belong to a facility in the same way, regardless of the source of the message (the Juniper Networks routing platform or the remote machine itself). For example, the following statements in the configuration of the routing platform called local-router direct messages from the authorization facility to the remote machine monitor.mycompany.com:

```
[edit system syslog]
host monitor.mycompany.com {
    authorization info;
}
```

The default alternative facility for the local authorization facility is also authorization. If the syslogd utility on monitor is configured to write messages belonging to the authorization facility to the file /var/log/auth-attempts, the file contains both the messages generated when users log in to local-router and the messages generated when users log in to monitor. Although the name of the source machine appears in

each system log message, the mixing of messages from multiple machines can make it more difficult to analyze the contents of the auth-attempts file.

To make it easier to separate the messages from each source, you can assign an alternative facility to all messages generated on local-router when they are directed to monitor. You can then configure the syslogd utility on monitor to write messages with the alternative facility to a different file from messages generated on monitor itself.

To change the facility used for all messages directed to a remote machine, include the facility-override statement at the [edit system syslog host *hostname*] hierarchy level:

```
[edit system syslog host hostname]
facility severity;
facility-override facility;
```

In general, it makes sense to specify an alternative facility that is not already in use on the remote machine, such as one of the local*X* facilities. On the remote machine, you must also configure the syslogd utility to handle the messages in the desired manner.

Table 22 on page 121 lists the facilities that you can specify in the facility-override statement.

**Table 22: Facilities for the facility-override Statement**

| Facility | Description |
|---|---|
| authorization | Authentication and authorization attempts |
| daemon | Actions performed or errors encountered by system processes |
| ftp | Actions performed or errors encountered by the FTP process |
| kernel | Actions performed or errors encountered by the JUNOS kernel |
| local0 | Local facility number 0 |
| local1 | Local facility number 1 |
| local2 | Local facility number 2 |
| local3 | Local facility number 3 |
| local4 | Local facility number 4 |
| local5 | Local facility number 5 |
| local6 | Local facility number 6 |
| local7 | Local facility number 7 |
| user | Actions performed or errors encountered by user-space processes |

We do not recommend including the facility-override statement at the [edit system syslog host other-routing-engine] hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its JUNOS system logging utility can interpret the JUNOS software-specific names.

#### *Examples: Assigning an Alternative Facility*

Log all messages generated on the local routing platform at the error level or higher to the local0 facility on the remote machine called monitor.mycompany.com:

```
[edit system syslog]
host monitor.mycompany.com {
    any error;
    facility-override local0;
}
```

Configure routing platforms located in California and routing platforms located in New York to send messages to a single remote machine called central-logger.mycompany.com. The messages from California are assigned alternative facility local0 and the messages from New York are assigned to alternative facility local2.

- Configure California routing platforms to aggregate messages in the local0 facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
      change-log info;
      facility-override local0;
  }
  ```

- Configure New York routing platforms to aggregate messages in the local2 facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
      change-log info;
      facility-override local2;
  }
  ```

On central-logger, you can then configure the system logging utility to write messages from the local0 facility to the file california-config and the messages from the local2 facility to the file new-york-config.

### Adding a Text String to System Log Messages

To add a text string to every system log message directed to a remote machine or to the other Routing Engine, include the log-prefix statement at the [edit system syslog host] hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
log-prefix string;
```

The string can contain any alphanumeric or special character except the equal sign ( = ) and the colon ( : ). It also cannot include the space character; do not enclose the string in quotation marks (“ ”) in an attempt to include spaces in it.

The JUNOS system logging utility automatically appends a colon and a space to the specified string when the system log messages are written to the log. The string is inserted after the identifier for the Routing Engine that generated the message.

#### *Example: Adding a String*

Add the string M120 to all messages to indicate that the router is an M120 router, and direct the messages to the remote machine hardware-logger.mycompany.com:

```
[edit system syslog]
host hardware-logger.mycompany.com {
    any info;
    log-prefix M120;
}
```

When these configuration statements are included on an M120 router called origin1, a message in the system log on hardware-logger.mycompany.com looks like the following:

```
Mar 9 17:33:23 origin1 M120: mgd[477]: UI_CMDLINE_READ_LINE: user ‘root’,
    command ‘run show version’
```

### *Specifying Log File Size, Number, and Archiving Properties*

To prevent log files from growing too large, the JUNOS system logging utility by default writes messages to a sequence of files of a defined size. The files in the sequence are referred to as *archive* files to distinguish them from the *active* file to which messages are currently being written. The default maximum size depends on the platform type:

- 128 kilobytes (KB) for J-series Services Routers
- 1 (MB) for M-series, MX-series, and T-series routing platforms
- 10 MB for TX Matrix platforms

When an active log file called *logfile* reaches the maximum size, the logging utility closes the file, compresses it, and names the compressed archive file *logfile*.0.gz. The logging utility then opens and writes to a new active file called *logfile*. When the new *logfile* reaches the configured maximum size, *logfile*.0.gz is renamed *logfile*.1.gz, and the new *logfile* is closed, compressed, and renamed *logfile*.0.gz. By default, the logging utility creates up to 10 archive files in this manner. When the maximum number of archive files is reached, each time the active file reaches the maximum size the contents of the oldest archive file are overwritten by the next oldest file. The logging utility by default also limits the users who can read log files to the root user and users who have the JUNOS maintenance permission.

You can include the archive statement to change the maximum size of each file, how many archive files are created, and who can read log files.

To configure values that apply to all log files, include the archive statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
archive {
    files number;
    size size;
    (world-readable | no-world-readable);
}
```

To configure values that apply to a specific log file, include the archive statement at the [edit system syslog file *filename*] hierarchy level:

```
[edit system syslog file filename]
facility severity;
archive {
    archive-sites {
        site-name;
    }
    files number;
    size size;
    start-time date.time;
    transfer-interval interval;
    (world-readable | no-world-readable);
}
```

archive-sites *site-name* specifies a list of archive sites that you want to use for storing files. The *site-name* value is any valid FTP URL to a destination. If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the specified log file name. For information about how to specify valid FTP URLs, see "Specifying Filenames and URLs" on page 36.

files *number* specifies the number of files to create before the oldest file is overwritten. The value can be from 1 through 1000.

size *size* specifies the maximum size of each file. The value can be from 64 KB (64k) through 1 gigabyte (1g); to represent megabytes, use the letter m after the integer. There is no space between the digits and the k, m, or g units letter.

start-time *date.time* defines the day and time at which you want the file transfer to occur. The format for *date.time* is yyyy-mm-dd.hh:mm. This is a one-time file transfer of the active log file to one of the specified archive sites.

transfer-interval *interval* defines the amount of time the current log file remains open (even if it has not reached the maximum possible size) and receives new statistics before it is closed and transferred to an archive site. This interval value can be from 5 through 2880 minutes.

world-readable enables all users to read log files. To restore the default permissions, include the no-world-readable statement.

### *Including Priority Information in System Log Messages*

A message's facility and severity level are together referred to as its *priority*. By default, messages logged in the standard JUNOS format do not include information about priority. To include priority information in standard-format messages directed to a file, include the explicit-priority statement at the [edit system syslog file *filename*] hierarchy level:

```
[edit system syslog file filename]
facility severity;
explicit-priority;
```

**NOTE:** Messages logged in structured-data format include priority information by default (structured-data format is available in JUNOS Release 8.3 and later and for file destinations only). If you include the structured-data statement at the [edit system syslog file *filename*] hierarchy level along with the explicit-priority statement, the explicit-priority statement is ignored and messages are logged in structured-data format.

For information about the structured-data statement, see "Logging Messages in Structured-Data Format" on page 117. For information about the contents of a structured-data message, see the *JUNOS System Log Messages Reference*.

To include priority information in messages directed to a remote machine or the other Routing Engine, include the explicit-priority statement at the [edit system syslog host (*hostname* | other-routing-engine)] hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
explicit-priority;
```

The priority recorded in a message always indicates the original, local facility name. If the facility-override statement is included for messages directed to a remote destination, the JUNOS system logging utility still uses the alternative facility name for the messages themselves when directing them to the remote destination. For more information, see "Changing the Alternative Facility Name for Remote Messages" on page 120.

When the explicit-priority statement is included, the JUNOS logging utility prepends codes for the facility name and severity level to the message tag name, if the message has one:

*FACILITY*-*severity*[-*TAG*]

(The tag is a unique identifier assigned to some JUNOS system log messages; for more information, see the *JUNOS System Log Messages Reference*.)

Table 23 on page 126 lists the facility codes that can appear in system log messages and maps them to facility names.

**NOTE:** If the second column in Table 23 on page 126 does not include the JUNOS facility name for a code, the facility cannot be included in a statement at the [edit system syslog] hierarchy level. The JUNOS software might use the facilities in Table 23 on page 126—and others that are not listed—when reporting on internal operations.

**Table 23: Facility Codes Reported in Priority Information**

| Code | JUNOS Facility Name | Type of Event or Error |
|---|---|---|
| AUTH | authorization | Authentication and authorization attempts |
| AUTHPRIV | | Authentication and authorization attempts that can be viewed by superusers only |
| CHANGE | change-log | Changes to the JUNOS configuration |
| CONFLICT | conflict-log | Specified configuration is invalid on the routing platform type |
| CONSOLE | | Messages written to /dev/console by the kernel console output r |
| CRON | | Actions performed or errors encountered by the cron process |
| DAEMON | daemon | Actions performed or errors encountered by system processes |
| DFC | dfc | Actions performed or errors encountered by the dynamic flow capture process |
| FIREWALL | firewall | Packet filtering actions performed by a firewall filter |
| FTP | ftp | Actions performed or errors encountered by the FTP process |
| INTERACT | interactive-commands | Commands issued at the JUNOS CLI prompt or invoked by a client application such as a JUNOScript or NETCONF client |
| KERN | kernel | Actions performed or errors encountered by the JUNOS kernel |
| NTP | | Actions performed or errors encountered by the Network Time Protocol (NTP) |
| PFE | pfe | Actions performed or errors encountered by the Packet Forwarding Engine |
| SYSLOG | | Actions performed or errors encountered by the JUNOS system logging utility |
| USER | user | Actions performed or errors encountered by user-space processes |

Table 24 on page 127 lists the numerical severity codes that can appear in system log messages and maps them to severity levels.

**Table 24: Numerical Codes for Severity Levels Reported in Priority Information**

| Numerical Code | Severity Level | Description |
|---|---|---|
| 0 | emergency | System panic or other condition that causes the routing platform to stop functioning |
| 1 | alert | Conditions that require immediate correction, such as a corrupted system database |
| 2 | critical | Critical conditions, such as hard errors |
| 3 | error | Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels |
| 4 | warning | Conditions that warrant monitoring |
| 5 | notice | Conditions that are not errors but might warrant special handling |
| 6 | info | Events or nonerror conditions of interest |
| 7 | debug | Software debugging messages (these appear only if a technical support representative has instructed you to configure this severity level) |

In the following example, the CHASSISD_PARSE_COMPLETE message belongs to the daemon facility and is assigned severity info (6):

```
Aug 21 12:36:30 router1 chassisd[522]: %DAEMON-6-CHASSISD_PARSE_COMPLETE:
    Using new configuration
```

When the explicit-priority statement is not included, the priority does not appear in the message:

```
Aug 21 12:36:30 router1 chassisd[522]: CHASSISD_PARSE_COMPLETE: Using new
    configuration
```

For more information about message formatting, see the *JUNOS System Log Messages Reference*.

## *Including the Year or Millisecond in Timestamps*

By default, the timestamp recorded in a standard-format system log message specifies the month, date, hour, minute, and second when the message was logged, as in the following example:

```
Aug 21 12:36:30
```

To include the year, the millisecond, or both in the timestamp, include the time-format statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
time-format (year | millisecond | year millisecond);
```

The modified timestamp is used in messages directed to each destination configured by a file, console, or user statement at the [edit system syslog] hierarchy level, but not to destinations configured by a host statement.

The following example illustrates the format for a timestamp that includes both the millisecond (401) and the year (2006):

```
Aug 21 12:36:30.401 2006
```

**NOTE:** Messages logged in structured-data format (available in JUNOS Release 8.3 and later for file destinations) include the year and millisecond by default. If you include the structured-data statement at the [edit system syslog file *filename*] hierarchy level along with the time-format statement, the time-format statement is ignored and messages are logged in structured-data format.

For information about the structured-data statement, see "Logging Messages in Structured-Data Format" on page 117. For information about the contents of a structured-data message, see the *JUNOS System Log Messages Reference*.

### *Using Regular Expressions to Refine the Set of Logged Messages*

The predefined facilities group together related messages, but you can also use regular expression matching to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination.

To specify the text string that must (or must not) appear in a message for the message to be logged to a destination, include the match statement and specify the regular expression which the text string must match:

```
match "regular-expression";
```

You can include this statement at the following hierarchy levels:

- [edit system syslog file *filename*] (for a file)
- [edit system syslog user (*username* | *)] (for the terminal session of one or all users)
- [edit system syslog host (*hostname* | other-routing-engine)] (for a remote destination)

In specifying the regular expression, use the notation defined in POSIX Standard 1003.2 for extended (modern) UNIX regular expressions. Explaining regular expression syntax is beyond the scope of this document, but POSIX standards are available from the Institute of Electrical and Electronics Engineers (IEEE, http://www.ieee.org).

Table 25 on page 129 specifies which character or characters are matched by some of the regular expression operators that you can use in the match statement. In the descriptions, the term *term* refers to either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.

**NOTE:** The match statement is not case-sensitive.

**Table 25: Regular Expression Operators for the match Statement**

| Operator | Matches |
|---|---|
| . (period) | One instance of any character except the space. |
| * (asterisk) | Zero or more instances of the immediately preceding term. |
| + (plus sign) | One or more instances of the immediately preceding term. |
| ? (question mark) | Zero or one instance of the immediately preceding term. |
| \| (pipe) | One of the terms that appear on either side of the pipe operator. |
| ! (exclamation point) | Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is JUNOS software-specific. |
| ^ (caret) | The start of a line, when the caret appears outside square brackets.<br><br>One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets. |
| $ (dollar sign) | The end of a line. |
| [ ] (paired square brackets) | One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen ( - ) to separate the beginning and ending characters of the range. For example, [a-z0-9] matches any letter or number. |
| ( ) (paired parentheses) | One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression. |

### Example: Using Regular Expressions

Filter messages that belong to the interactive-commands facility, directing those that include the string configure to the terminal of the root user:

```
[edit system syslog]
user root {
    interactive-commands any;
    match ".*configure.*";
}
```

Messages like the following appear on the root user's terminal when a user issues a configure command to enter configuration mode:

*timestamp router-name* mgd[*PID*]: UI_CMDLINE_READ_LINE: User '*user*', command 'configure private'

Filter messages that belong to the daemon facility and have severity error or higher, directing them to the file /var/log/process-errors. Omit messages generated by the SNMP process (snmpd), instead directing them to the file /var/log/snmpd-errors:

```
[edit system syslog]
file process-errors {
    daemon error;
    match "!(.*snmpd.*)";
}
file snmpd-errors {
    daemon error;
    match ".*snmpd.*";
}
```

### Disabling Logging of a Facility

To disable the logging of messages that belong to a particular facility, include the *facility* none statement in the configuration. This statement is useful when, for example, you want to log messages that have the same severity level and belong to all but a few facilities. Instead of including a statement for each facility you want to log, you can include the any *severity* statement and then a *facility* none statement for each facility that you do not want to log. For example, the following logs all messages at the error level or higher to the console, except for messages from the daemon and kernel facilities. Messages from those facilities are logged to the file >/var/log/internals instead:

```
[edit system syslog]
console {
    any error;
    daemon none;
    kernel none;
}
file internals {
    daemon info;
    kernel info;
}
```

### Examples: Configuring System Logging

Log messages about all commands entered by users at the CLI prompt or invoked by client applications such as JUNOScript or NETCONF client applications, and all authentication or authorization attempts, both to the file cli-commands and to the terminal of any user who is logged in:

```
[edit system]
syslog {
    file cli-commands {
        interactive-commands info;
        authorization info;
    }
    user * {
        interactive-commands info;
        authorization info;
    }
```

```
}
```

Log all changes in the state of alarms to the file /var/log/alarms:

```
[edit system]
syslog {
    file alarms {
        kernel warning;
    }
}
```

Configure the handling of messages of various types, as described in the comments. Information is logged to two files, to the terminal of user alex, to a remote machine, and to the console:

```
[edit system]
syslog {
    /* write all security-related messages to file /var/log/security */
    file security {
        authorization info;
        interactive-commands info;
    }
    /* write messages about potential problems to file /var/log/messages: */
    /* messages from "authorization" facility at level "notice" and above, */
    /* messages from all other facilities at level "warning" and above */
    file messages {
        authorization notice;
        any warning;
    }
    /* write all messages at level "critical" and above to terminal of user "alex" if */
    /* that user is logged in */
    user alex {
        any critical;
    }
    /* write all messages from the "daemon" facility at level "info" and above, and */
    /* messages from all other facilities at level "warning" and above, to the */
    /* machine monitor.mycompany.com */
    host monitor.mycompany.com {
        daemon info;
        any warning;
    }
    /* write all messages at level "error" and above to the system console */
    console {
        any error;
    }
}
```

Configure the handling of messages generated when users issue JUNOS CLI commands, by specifying the interactive-commands facility at the following severity levels:

- info—Logs a message when users issue any command at the CLI operational or configuration mode prompt. The example writes the messages to the file /var/log/user-actions.

- notice—Logs a message when users issue the configuration mode commands rollback and commit. The example writes the messages to the terminal of user philip.
- warning—Logs a message when users issue a command that restarts a software process. The example writes the messages to the console.

```
[edit system]
syslog {
    file user-actions {
        interactive-commands info;
    }
    user philip {
        interactive-commands notice;
    }
    console {
        interactive-commands warning;
    }
}
```

## Configuring System Logging for a Routing Matrix

This section explains how to configure system logging for the T640 Internet routing nodes and TX Matrix platform in a routing matrix. It assumes you are familiar with system logging for single-chassis systems, as described in "Configuring System Logging for a Single-Chassis System" on page 113. For more information about routing matrixes, see *TX Matrix Platform Hardware Guide*.

To configure system logging for all platforms in a routing matrix, include the syslog statement at the [edit system] hierarchy level on the TX Matrix platform. The syslog statement applies to every platform in the routing matrix.

```
[edit system]
syslog {
    archive {
        files number;
        size size;
        (world-readable | no-world-readable);
    }
    console {
        facility severity;
    }
    file filename {
        facility severity;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
        archive {
            files number;
            size size;
            (world-readable | no-world-readable);
        }
```

```
    }
    host (hostname | other-routing-engine | scc-master) {
      facility severity;
      explicit-priority;
      facility-override facility;
      log-prefix string;
      match "regular-expression";
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
      facility severity;
      match "regular-expression";
    }
  }
```

When included in the configuration on the TX Matrix platform, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every platform in the routing matrix:

- archive—Sets the size and number of log files on each platform in the routing matrix. See "Specifying Log File Size, Number, and Archiving Properties" on page 123.
- console—Directs the specified messages to the console of each platform in the routing matrix. See "Directing Messages to the Console" on page 118.
- file—Directs the specified messages to a file of the same name on each platform in the routing matrix. See "Directing Messages to a Log File" on page 116.
- match—Limits the set of messages logged to a destination to those that contain (or do not contain) a text string matching a regular expression. See "Using Regular Expressions to Refine the Set of Logged Messages" on page 128.

  The separate match statement at the [edit system syslog host scc-master] hierarchy level applies to messages forwarded from the T640 routing nodes to the TX Matrix platform. See "Configuring Optional Features for Forwarded Messages" on page 137.
- source-address—Sets the IP address of the routing platform to report in system log messages as the message source, when the messages are directed to the remote machines specified in all host *hostname* statements at the [edit system syslog] hierarchy level, for each platform in the routing matrix. The address is not reported in messages directed to the other Routing Engine on each platform or to the TX Matrix platform by the T640 routing nodes. See "Specifying an Alternative Source Address for System Log Messages" on page 119.
- structured-data—Writes messages to a file in structured-data format. See "Logging Messages in Structured-Data Format" on page 117.
- time-format—Adds the millisecond, year, or both to the timestamp in each standard-format message. See "Including the Year or Millisecond in Timestamps" on page 127.
- user—Directs the specified messages to the terminal session of one or more specified users on each platform in the routing matrix that they are logged in to. See "Directing Messages to a User Terminal" on page 118.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system. For more information, see the following sections:



### *Configuring Message Forwarding in the Routing Matrix*

By default, the master Routing Engine on each T640 routing node forwards to the master Routing Engine on the TX Matrix platform all messages from all facilities with severity level of info and higher. To change the facility, the severity level, or both, include the host scc-master statement at the [edit system syslog] hierarchy level on the TX Matrix platform:

```
[edit system syslog]
host scc-master {
    facility severity;
}
```

To disable message forwarding, set the facility to any and the severity level to none:

```
[edit system syslog]
host scc-master {
    any none;
}
```

In either case, the setting applies to all T640 routing nodes in the routing matrix.

To capture the messages forwarded by the T640 routing nodes (as well as messages generated on the TX Matrix platform itself), you must also configure system logging on the TX Matrix platform. Direct the messages to one or more destinations by including the appropriate statements at the [edit system syslog] hierarchy level on the TX Matrix platform:

- To a file, as described in "Directing Messages to a Log File" on page 116.
- To the terminal session of one or more specific users (or all users), as described in "Directing Messages to a User Terminal" on page 118.
- To the console, as described in "Directing Messages to the Console" on page 118.
- To a remote machine that is running the syslogd utility or to the other Routing Engine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix" on page 138.

As previously noted, the configuration statements included on the TX Matrix platform also configure the same destinations on each T640 routing node.

When specifying the severity level for local messages (at the [edit system syslog (file | host | console | user)] hierarchy level) and forwarded messages (at the [edit system syslog host scc-master] hierarchy level), you can set the same severity level for both, set a lower severity level for local messages, or set a higher severity

level for local messages. The following examples describe the consequence of each configuration. (For simplicity, the examples use the any facility in every case. You can also specify different severities for different facilities, with more complex consequences.)

- Messages Logged When Local and Forwarded Severity Levels Are the Same on page 135
- Messages Logged When Local Severity Level Is Lower on page 135
- Messages Logged When Local Severity Level Is Higher on page 136

### Messages Logged When Local and Forwarded Severity Levels Are the Same

When the severity level is the same for local and forwarded messages, the log on the TX Matrix platform contains all messages from the logs on the T640 routing nodes. For example, you can specify severity info for the /var/log/messages file, which is the default severity level for messages forwarded by T640 routing nodes:

```
[edit system syslog]
file messages {
    any info;
}
```

Table 26 on page 135 specifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform.

**Table 26: Example: Local and Forwarded Severity Level Are Both info**

| Log Location | Source of Messages | Lowest Severity Included |
|---|---|---|
| T640 routing node | Local | info |
| TX Matrix platform | Local | info |
| | Forwarded from T640 routing nodes | info |

### Messages Logged When Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix platform includes fewer forwarded messages than when the severities are the same. Locally generated messages are still logged at the lower severity level, so their number in each log is the same as when the severities are the same.

For example, you can specify severity notice for the /var/log/messages file and severity critical for forwarded messages:

```
[edit system syslog]
file messages {
    any notice;
}
host scc-master {
    any critical;
```

```
}
```

Table 27 on page 136 specifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform. The T640 routing nodes forward only those messages with severity critical and higher, so the log on the TX Matrix platform does not include the messages with severity error, warning, or notice that the T640 routing nodes log locally.

**Table 27: Example: Local Severity Is notice, Forwarded Severity Is critical**

| Log Location | Source of Messages | Lowest Severity Included |
|---|---|---|
| T640 routing node | Local | notice |
| TX Matrix platform | Local | notice |
| | Forwarded from T640 routing nodes | critical |

## Messages Logged When Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix platform includes fewer forwarded messages than when the severities are the same, and all local logs contain fewer messages overall.

For example, you can specify severity critical for the /var/log/messages file and severity notice for forwarded messages:

```
[edit system syslog]
file messages {
    any critical;
}
host scc-master {
    any notice;
}
```

Table 28 on page 136 specifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform. Although the T640 routing nodes forward messages with severity notice and higher, the TX Matrix platform discards any of those messages with severity critical or lower (does not log forwarded messages with severity error, warning, or notice). None of the logs include messages with severity error or lower.

**Table 28: Example: Local Severity Is critical, Forwarded Severity Is notice**

| Log Location | Source of Messages | Lowest Severity Included |
|---|---|---|
| T640 routing node | Local | critical |
| TX Matrix platform | Local | critical |
| | Forwarded from T640 routing nodes | critical |

## *Configuring Optional Features for Forwarded Messages*

To configure additional optional features when specifying how the T640 routing nodes forward messages to the TX Matrix platform, include statements at the [edit system syslog host scc-master] hierarchy level. To include priority information (facility and severity level) in each forwarded message, include the explicit-priority statement. To insert a text string in each forwarded message, include the log-prefix statement. To use regular expression matching to specify more exactly which messages from a facility are forwarded, include the match statement.

```
[edit system syslog]
host scc-master {
    facility severity;
    explicit-priority;
    log-prefix string;
    match "regular-expression;
}
```

**NOTE:** You can also include the facility-override statement at the [edit system syslog host scc-master] hierarchy level, but we do not recommend doing so. It is not necessary to use alternative facilities for messages forwarded to the TX Matrix platform, because it runs the JUNOS system logging utility and can interpret the JUNOS software-specific facilities. For more information about alternative facilities, see "Changing the Alternative Facility Name for Remote Messages" on page 120.

### Including Priority Information in Forwarded Messages

When you include the explicit-priority statement at the [edit system syslog host scc-master] hierarchy level, messages forwarded to the TX Matrix platform include priority information. For the information to appear in a log file on the TX Matrix platform, you must also include the explicit-priority statement at the [edit system syslog file *filename*] hierarchy level for the file on the TX Matrix platform. As a consequence, the log file with the same name on each platform in the routing matrix also includes priority information for locally generated messages.

To include priority information in messages directed to a remote machine from all platforms in the routing matrix, also include the explicit-priority statement at the [edit system syslog host *hostname*] hierarchy level for the remote machine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix" on page 138.

In the following example, the /var/log/messages file on all platforms includes priority information for messages with severity notice and higher from all facilities. The log on the TX Matrix platform also includes messages with those characteristics forwarded from the T640 routing nodes.

```
[edit system syslog]
host scc-master {
    any notice;
    explicit-priority;
}
```

```
file messages {
    any notice;
    explicit-priority;
}
```

### Adding a Text String to Forwarded Messages

When you include the log-prefix statement at the [edit system syslog host scc-master] hierarchy level, the string that you define appears in every message forwarded to the TX Matrix platform. For more information, see "Adding a Text String to System Log Messages" on page 122.

### Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the match statement [edit system syslog host scc-master] hierarchy level, the regular expression that you specify controls which messages from the T640 routing nodes are forwarded to the TX Matrix platform. The regular expression is not applied to messages from the T640 routing notes that are directed to destinations other than the TX Matrix platform. For more information about regular expression matching, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 128.

## *Directing Messages to a Remote Destination from the Routing Matrix*

You can configure a routing matrix to direct system logging messages to a remote machine or the other Routing Engine on each routing platform, just as on a single-chassis system. Include the host statement at the [edit system syslog] hierarchy level on the TX Matrix platform:

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
}
source-address source-address;
```

The TX Matrix platform directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional statements (explicit-priority, facility-override, log-prefix, match, and source-address) also have the same effect as on a single-chassis system. For more information, see "Directing Messages to a Remote Machine or the Other Routing Engine" on page 118.

For the TX Matrix platform to include priority information when it directs messages that originated on a T640 routing node to the remote destination, you must also include the explicit-priority statement at the [edit system syslog host scc-master] hierarchy level.

The other-routing-engine statement does not interact with message forwarding from the T640 routing nodes to the TX Matrix platform. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (re0), the re0 Routing

Engine on each T640 routing node sends messages to the re1 Routing Engine on its platform only. It does not also send messages directly to the re1 Routing Engine on the TX Matrix platform.

Because the configuration on the TX Matrix platform applies to the T640 routing nodes, any T640 routing node that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the T640 routing nodes are configured to forward messages to the TX Matrix platform (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T640 routing node and the other from the TX Matrix platform. Which messages are duplicated depends on whether the severities are the same for local logging and for forwarded messages. For more information, see "Configuring Message Forwarding in the Routing Matrix" on page 134.
- If the source-address statement is configured at the [edit system syslog] hierarchy level, all platforms in the routing matrix report the same source address in messages directed to the remote machine. This is appropriate, because the routing matrix functions as a single routing platform.
- If the log-prefix statement is included, the messages from all platforms in the routing matrix include the same text string. You cannot use the string to distinguish between the platforms in the routing matrix.

### *Configuring System Logging Differently on Each Platform*

We recommend that all platforms in a routing matrix use the same configuration, which implies that you include system logging configuration statements on the TX Matrix platform only. In rare circumstances, however, you might choose to log different messages on different platforms. For example, if one platform in the routing matrix is experiencing problems with authentication, a Juniper Networks support representative might instruct you to log messages from the authorization facility with severity debug on that platform.

To configure platforms separately, include configuration statements in the appropriate groups at the [edit groups] hierarchy level on the TX Matrix platform:

- To configure settings that apply to the TX Matrix platform but not the T640 routing nodes, include them in the re0 and re1 configuration groups.
- To configure settings that apply to particular T640 routing nodes, include them in the lcc*n*-re0 and lcc*n*-re1 configuration groups, where *n* is the line-card chassis (LCC) index number of the routing node.

When you use configuration groups, do not issue CLI configuration-mode commands to change statements at the [edit system syslog] hierarchy level on the TX Matrix platform. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T640 routing nodes also. (We further recommend that you do not issue CLI configuration-mode commands on the T640 routing nodes at any time.)

For more information about the configuration groups for a routing matrix, see the chapter about configuration groups in the *JUNOS CLI User Guide*.

The following example shows how to configure the /var/log/messages files on three platforms to include different sets of messages:

- On the TX Matrix platform, local messages with severity info and higher from all facilities. The file does not include messages from the T640 routing nodes, because the host scc-master statement disables message forwarding.
- On the T640 routing node designated LCC0, messages from the authorization facility with severity info and higher.
- On the T640 routing node designated LCC1, messages with severity notice from all facilities.

```
[edit groups]
re0 {
    system {
        syslog {
            file messages {
                any info;
            }
            host scc-master {
                any none;
            }
        }
    }
}
re1 {
    ... same statements as for re0 ...
}
lcc0-re0 {
    system {
        syslog {
            file messages {
                authorization info;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
    system {
        syslog {
            file messages {
                any notice;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc1-re0 ...
}
```

Chapter 10

# Configuring Miscellaneous System Management Features

This chapter discusses the following topics:

## Configuring Console and Auxiliary Port Properties

The router's craft interface has two ports—a console port and an auxiliary port—for connecting terminals to the router. The console port is enabled by default, and its speed is 9600 baud. The auxiliary port is disabled by default.

To configure the properties for the console and auxiliary ports, include the ports statement at the [edit system] hierarchy level:

```
[edit system]
ports {
    auxiliary {
        type terminal-type;
    }
    console {
        insecure;
        log-out-on-disconnect;
        type terminal-type;
        disable;
    }
}
```

By default, the terminal type is unknown, and the terminal speed is 9600 baud for both the console and auxiliary ports. To change the terminal type, include the type statement, specifying a *terminal-type* of ansi, vt100, small-xterm, or xterm. The first three terminal types set a screen size of 80 columns by 24 lines. The last type, xterm, sets the size to 80 columns by 65 rows.

By default, the console session is not logged out when the data carrier is lost on the console modem control lines. To log out the session when the data carrier on the console port is lost, include the log-out-on-disconnect statement.

By default, terminal connections to the console and auxiliary ports are secure. When you configure the console as insecure, root logins are not allowed to establish terminal connections. In addition, superusers and anyone with a user indentifier (UID) of 0

are not allowed to establish terminal connections in multiuser mode when you configure the console as insecure. To disable root login connections to the console and auxiliary ports, include the insecure statement.

To disable console login, include the disable statement. By default, console login is enabled.

For Common Criteria compliance the console port must be disabled. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

## Disabling the Sending of Redirect Messages on the Router

By default, the router sends protocol redirect messages. To disable the sending of redirect messages by the router, include the no-redirects statement at the [edit system] hierarchy level:

```
[edit system]
no-redirects;
```

To reenable the sending of redirect messages on the router, delete the no-redirects statement from the configuration.

To disable the sending of redirect messages on a per-interface basis, include the no-redirects statement at the [edit interfaces *interface-name* unit *logical-unit-number* family *family*] hierarchy level, as described in the *JUNOS Network Interfaces Configuration Guide*.

## Configuring the Source Address for Locally Generated TCP/IP Packets

By default, the source address included in locally generated Transmission Control Protocol/IP (TCP/IP) packets, such as FTP traffic, and in User Datagram Protocol (UDP) and IP packets, such as Network Time Protocol (NTP) requests, is chosen as the local address for the interface on which the traffic is transmitted. This means that the local address chosen for packets to a particular destination might change from connection to connection based on the interface that the routing protocol has chosen to reach the destination when the connection is established. If multiple equal-cost next hops are present for a destination, locally generated packets use the lo0 address as a source.

To configure the software to select a fixed address to use as the source for locally generated IP packets, include the default-address-selection statement at the [edit system] hierarchy level:

```
[edit system]
default-address-selection;
```

If you include the default-address-selection statement in the configuration, the JUNOS software chooses the system default address as the source for most locally generated IP packets. The default address is usually an address configured on the lo0 loopback interface. For example, if you specified that SSH and telnet use a particular address, but you also have default-address selection configured, the system default address is

used. For more information about how the default address is chosen, see the *JUNOS Network Interfaces Configuration Guide*.

For IP packets sent by IP routing protocols—including Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Resource Reservation Protocol (RSVP), and the multicast protocols, but not including Intermediate System-to-Intermediate System (IS-IS)—the local address selection is often constrained by the protocol specification so that the protocol operates correctly. When this constraint exists in the routing protocol, the packet's source address is unaffected by the presence of the default-address-selection statement in the configuration. For protocols in which the local address is unconstrained by the protocol specification, for example, internal Border Gateway Protocol (IBGP) and multihop external BGP (EBGP), if you do not configure a specific local address when configuring the protocol, the local address is chosen using the same method as other locally generated IP packets.

## Configuring the Router or Interface to Act as a DHCP/BOOTP Relay Agent

To configure a router or interface to act as a bootstrap protocol (DHCP/BOOTP) relay agent, you include statements at the [edit forwarding-options helpers] hierarchy level. For more information, see the *JUNOS Policy Framework Configuration Guide*.

For J-series Services Routers, you can configure a router or interface as a DHCP server by including statements at the [edit system services] hierarchy level. For more information, see "Configuring a DHCP Server" on page 147.

**NOTE:** You cannot configure a router or interface as a DHCP server and a BOOTP relay agent at the same time.

## Disabling the Response to Multicast Ping Packets

By default, the Routing Engine responds to Internet Control Message Protocol (ICMP) echo requests sent to multicast group addresses. To disable the Routing Engine from responding to ICMP echo requests sent to multicast group addresses, include the no-multicast-echo statement at the [edit system] hierarchy level:

```
[edit system]
no-multicast-echo;
```

By configuring the Routing Engine to ignore multicast ping packets, you can prevent unauthorized persons from discovering the list of provider edge (PE) routers in the network.

## Disabling the Reporting of IP Address and Timestamps in Ping Responses

By default, the Routing Engine displays the path of the ICMP echo request packets and timestamps in the ICMP echo responses when the ping command is issued with the record-route option.

You can configure the Routing Engine to disable the setting of the record-route option in the IP header of the ping request packets. Disabling the record-route option prevents the Routing Engine from recording and displaying the path of the ICMP echo request packets in the response.

To configure the Routing Engine to disable the setting of the record route option, include the no-ping-record-route statement at the [edit system] hierarchy level:

```
[edit system]
no-ping-record-route;
```

To disable the reporting of timestamps in the ICMP echo responses, include the no-ping-time-stamp option at the [edit system] hierarchy level:

```
[edit system]
no-ping-time-stamp;
```

By configuring the no-ping-record-route and no-ping-timestamp options, you can prevent unauthorized persons from discovering information about the provider edge (PE) router and its loopback address.

## Configuring System Services

For security reasons, remote access to the router is disabled by default. You must configure the router explicitly so that users on remote systems can access it. The router can be accessed from a remote system by means of the DHCP, finger, FTP, rlogin, SSH, and Telnet services. In addition, JUNOScript client applications can use Secure Sockets Layer (SSL) or the JUNOScript-specific clear-text service, among other services.

**NOTE:** To protect system resources, you can limit the number of simultaneous connections that a service accepts and the number of processes owned by a single user. If either limit is exceeded, connection attempts fail.

This section discusses the following topics:

Many JUNOS protocols and services cannot be configured on a router that runs the JUNOS-FIPS software, including DHCP, finger, FTP, JUNOScript clear-text, rlogin, rsh, and Telnet.

## *Configuring clear-text or SSL Service for JUNOScript Client Applications*

A JUNOScript client application can use one of four protocols to connect to the JUNOScript server on a router: clear-text (a JUNOScript-specific protocol for sending unencrypted text over a TCP connection), SSH, SSL, or Telnet. For clients to use the clear-text or SSL protocol, you must include JUNOScript-specific statements in the router configuration. For more information, see the following sections. For detailed information about configuring the four access protocols, see the *JUNOScript API Guide*.


- Configuring clear-text Service for JUNOScript Client Applications on page 146
- Configuring SSL Service for JUNOScript Client Applications on page 146


### Configuring clear-text Service for JUNOScript Client Applications

To configure the router to accept clear-text connections from JUNOScript client applications on port 3221, include the xnm-clear-text statement at the [edit system services] hierarchy level:

```
[edit system services]
xnm-clear-text {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

By default, the JUNOScript server supports a limited number of simultaneous clear-text sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- connection-limit *limit*—Maximum number of simultaneous connections (a value from 1 through 250). The default is 75.
- rate-limit *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.

You cannot include the xnm-clear-text statement on routers that run the JUNOS-FIPS software. We recommend that you do not use the clear-text protocol in a Common Criteria environment.

### Configuring SSL Service for JUNOScript Client Applications

To configure the router to accept SSL connections from JUNOScript client applications on port 3220, include the xnm-ssl statement at the [edit system services] hierarchy level:

```
[edit system services]
xnm-ssl {
    local-certificate name;
    <connection-limit limit>;
    <rate-limit limit>;
```

```
}
```

local-certificate is the name of the X.509 authentication certificate used to establish an SSL connection. You must obtain the certificate and copy it to the router before referencing it. For more information, see "Importing SSL Certificates for JUNOScript Support" on page 587.

By default, the JUNOScript server supports a limited number of simultaneous SSL sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- connection-limit *limit*—Maximum number of simultaneous connections (a value from 1 through 250). The default is 75.
- rate-limit *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.

## Configuring a DHCP Server

The Dynamic Host Configuration Protocol (DHCP) server provides a framework for passing configuration information to client hosts (such as PCs) on a TCP/IP network. A router or interface that acts as a DHCP server can allocate network IP addresses and deliver configuration settings to client hosts without user intervention. DHCP access service minimizes the overhead required to add clients to the network by providing a centralized, server-based setup. You do not have to manually create and maintain IP address assignments for clients. DHCP is defined in RFC 2131, *Dynamic Host Configuration Protocol*.

**NOTE:** The DHCP server is supported in J-series Services Routers and is compatible with the autoinstallation feature.

To configure a J-series Services Router to accept DHCP as an access service, include the dhcp statement at the [edit system services] hierarchy level:

```
[edit system services]
dhcp {
    boot-file filename;
    boot-server (address | hostname);
    domain-name domain-name;
    domain-search [domain-list];
    default-lease-time;
    maximum-lease-time;
    name-server {
        address;
    }
    option {
        [ (id-number option-type option-value) | (id-number array option-type option-value) ];
    }
    pool address/prefix-length) {
        address-range {
            low address;
            high address;
```

```
        }
        exclude-address {
            address;
        }
    }
    router {
        address;
    }
    static-binding mac-address {
        fixed-address {
            address;
        }
        host hostname;
        client-identifier (ascii client-id | hexadecimal client-id);
    }
    server-identifier address;
    wins-server {
        address;
    }
}
```

For information about configuring DHCP properties, see the following sections:



## DHCP Overview

DHCP access service consists of two components: a protocol for delivering host-specific configuration information from a server to a client host and a method for allocating network addresses to a client host. The client sends a message to request configuration information. A DHCP server sends the configuration information back to the client.

With DHCP, clients can be assigned a network address for a fixed *lease*, enabling serial reassignment of network addresses to different clients. A DHCP server leases IP addresses for specific times to various clients. If a client does not use its assigned

address for some period of time, the DHCP server can assign that IP address to another host. When assignments are made or changed, the DHCP server updates information in the DNS server. The DHCP server provides clients with their previous lease assignments whenever possible.

A DHCP server provides persistent storage of network parameters for clients. Because DHCP is an extension of BOOTP, DHCP servers can handle BOOTP requests.

The DHCP server includes IPv4 address assignment and commonly used DHCP options. The server is compatible with DHCP servers from other vendors on the network. The server does not support IPv6 address assignment, user class-specific configuration, DHCP failover protocol, dynamic DNS updates, or VPN connections. The JUNOS-FIPS software does not support the DHCP server.

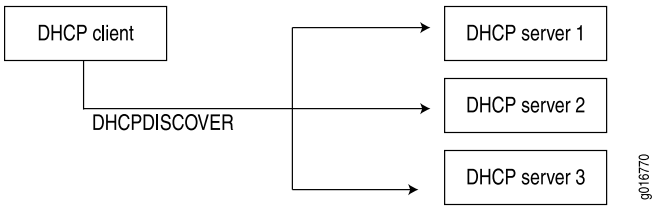
**NOTE:** You cannot configure a router as a DHCP server and a BOOTP relay agent at the same time.

### *Network Address Assignments (Allocating a New Address)*

To receive configuration information and a network address assignment, a DHCP client negotiates with DHCP servers in a series of messages. The following steps show the messages exchanged between a DHCP client and servers to allocate a new network address. When allocating a new network address, the DHCP process can involve more than one server, but only one server is selected by the client.

1. When a client computer is started, it broadcasts a DHCPDISCOVER message on the local subnet, requesting a DHCP server. This request includes the hardware address of the requesting client.

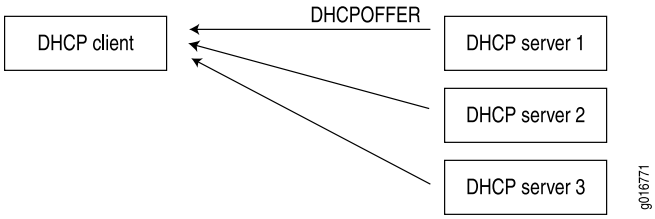
**Figure 4: DHCP Discover**




**NOTE:** For improved operation with DHCP clients that do not strictly conform to RFC 2131, the DHCP server accepts and processes DHCPDISCOVER messages even if the overload options in the messages are not properly terminated with an end statement.

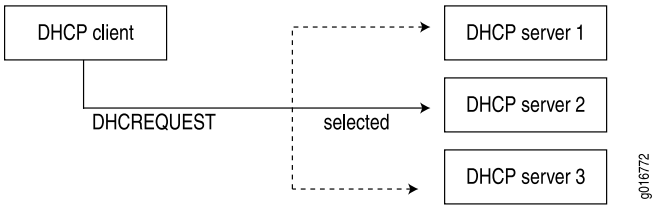
2. Each DHCP server receiving the broadcast sends a DHCPOFFER message to the client, offering an IP address for a set period of time, known as the lease period.

**Figure 5: DHCP Offer**



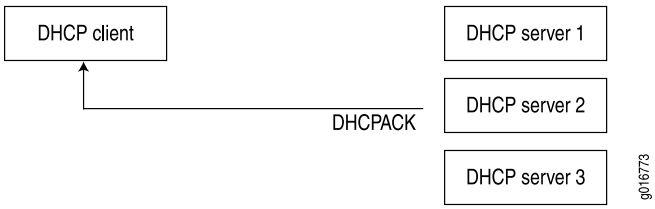

3. The client receives one or more DHCPOFFER messages from one or more servers and selects one of the offers received. Normally, a client looks for the longest lease period.
4. The client broadcasts a DHCPREQUEST message indicating the client has selected an offered leased IP address and identifies the selected server.

**Figure 6: DHCP Request**




5. Those servers not selected by the DHCPREQUEST message return the unselected IP addresses to the pool of available addresses.
6. The selected DHCP server sends a DHCPACK acknowledgment that includes configuration information such as the IP address, subnet mask, default gateway, and the lease period.

**Figure 7: DHCP ACK**

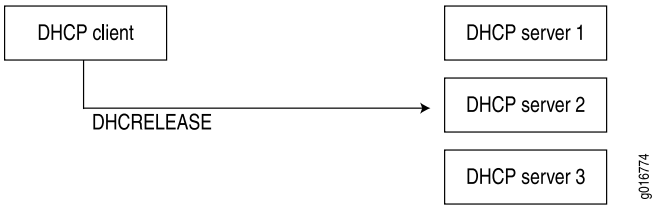



The information offered by the server is configurable. See “Configuring a DHCP Server” on page 147 for more information.

7. The client receives the DHCPACK message with configuration information. The process is complete. The client is configured and has access to the network.
   - If the client receives a DHCPNAK message (for example, if the client has moved to a new subnet), the client restarts the negotiation process.
   - The client can relinquish its lease on a network address by sending a DHCPRELEASE message to the server (for example, when the client is

restarted). When the server receives the DHCPRELEASE message, it marks the lease as free and the IP address becomes available again.

**Figure 8: DHCP Release**




### *Network Address Assignments (Reusing a Previously Assigned Address)*

To enable reuse of a previously allocated network address, the following events occur:

1. A client that previously had a lease broadcasts a DHCPREQUEST message on the local subnet.
2. The server with knowledge of the client's configuration responds with a DHCPACK message.
3. The client verifies the DHCP configuration information sent by the server and uses this information to reestablish the lease.

### *Static and Dynamic Bindings*

DHCP supports both dynamic and static bindings. For dynamic bindings, IP addresses are assigned to clients from a pool of addresses. Static bindings provide configuration information for a specific client and can include one or more fixed IP addresses for the client. You can configure a DHCP server to include both address pools and static bindings. For any individual client, static bindings take priority over address pools.

### *Compatibility with Autoinstallation*

The DHCP server is compatible with the autoinstallation feature on J-series Services Routers. The server automatically checks autoinstallation settings for conflicts and gives autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes priority over an IP address set by the DHCP server.

**NOTE:** The autoinstallation feature includes a fixed address pool and a fixed lease time. With DHCP, you can create address pools and modify lease times.

### *Conflict Detection and Resolution*

When a client receives an IP address from the DHCP server, the client performs a series of ARP tests to verify that the IP address is available and no conflicts exist. If

the client detects an address conflict, the client notifies the DHCP server about the conflict and may request another IP address from the DHCP server.

The DHCP server keeps a log of all conflicts and removes addresses with conflicts from the pool. These addresses remain excluded until you manually clear the conflicts list with the clear system services dhcp conflict command. For more information on this command, see the *JUNOS System Basics and Services Command Reference*.

### *DHCP Statement Hierarchy and Inheritance*

DHCP configuration statements are organized hierarchically. Statements at the top of the hierarchy apply to the DHCP server and network, branches contain statements that apply to address pools in a subnetwork, and leaves contain statements that apply to static bindings for individual clients. See Table 29 on page 152.

The pool and static-binding statements appear at the [edit system services dhcp] hierarchy level. You can include the remaining statements at the following hierarchy levels:

[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]

**Table 29: Pool and Binding Statements**

| Statement | Description | Hierarchy Level |
|---|---|---|
| pool | Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool. | [edit system services dhcp] |
| static-binding | Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address. | |

To minimize configuration changes, include common configuration statements shown in Table 30 on page 153 (for example, the domain-name statement) at the highest applicable level of the hierarchy (network or subnetwork). Configuration statements at lower levels of the hierarchy override statements inherited from a higher level. For example, if a statement appears at both the [edit system services dhcp] and [edit system services dhcp pool] hierarchy levels, the value assigned to the statement at the [edit system services dhcp pool] level takes priority.

**Table 30: Common Configuration Statements**

| Statement | Description | Hierarchy Level |
|---|---|---|
| boot-file | Set the boot filename advertised to clients. The client uses the boot image stored in the boot file to complete configuration. | [edit system services dhcp]<br>[edit system services dhcp pool]<br>[edit system services dhcp static-binding] |
| boot-server | Set the server that contains the boot file. | |
| default-lease-time | Set the default lease time assigned to any client that does not request a specific lease time. | |
| domain-name | Configure the name of the domain in which clients will search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. | |
| domain-search | Define a domain search list. | |
| maximum-lease-time | Set the maximum lease time allowed by the server. | |
| name-server | Specify the DNS server that maintains the database of client name to IP address mappings. | |
| option | Configure user-defined DHCP options. | |
| router | Specify IP address for routers on the client's subnetwork. Routers are listed in order of preference. | |
| server-identifier | Set the IP address of the DHCP server. | |

## Configuring Address Pools

For dynamic bindings, set aside a pool of IP addresses that can be assigned to clients. Addresses in a pool must be available to clients on the same subnet.

To configure an address pool, include the following statements at the [edit system services dhcp] hierarchy level:

```
[edit system services dhcp]
pool (***address/prefix-length) {
    address-range {
        low address;
        high address;
    }
```

```
    exclude-address {
      address;
    }
  }
```

The pool definition must include the client subnet number and prefix length (in bits). Optionally, the definition can include an address range and a list of excluded addresses.

The address-range statement defines the lowest and highest IP addresses in the pool that are available for dynamic address assignment. This statement is optional. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

The exclude-address statement specifies addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range. This statement is optional.

The following is an example of a pool configuration.

```
[edit system services dhcp]
pool 10.3.3.0/24 {
  address-range low 10.3.3.2 high 10.3.3.254;
  exclude-address {
    10.3.3.33;
  }
}
```

For dynamic address assignment, configure an address pool for each client subnet the DHCP server supports. You can configure multiple address pools for a DHCP server, but only one address range per pool is supported.

DHCP maintains the state information for all pools configured. Clients are assigned addresses from pools with subnets that match the interface on which the DHCPDISCOVER packet is received. When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.

### Configuring Manual (Static) Bindings

Static bindings provide configuration information for specific clients. This information can include one or more fixed Internet addresses, the client hostname, and a client identifier.

To configure static bindings, include the following statements at the [edit system services dhcp] hierarchy level:

```
[edit system services dhcp]
static-binding mac-address {
  fixed-address {
    address;
  }
  host client-hostname;
  client-identifier (ascii client-id | hexadecimal client-id);
}
```

A static binding defines a mapping between a fixed IP address and the client's MAC address.

The *mac-address* variable specifies the MAC address of the client. This is a hardware address that uniquely identifies each client on the network.

The fixed-address statement specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

The host statement specifies the hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the domain-name statement.

The client-identifier statement is used by the DHCP server to index the database of address bindings. The client identifier is either an ASCII string or hexadecimal digits. It can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

**NOTE:** For each unique client-identifier *client-id* value, the DHCP server issues a unique lease and IP address from the pool. Previously, when the client provided an incorrect client-identifier *client-id* value, the DHCP server did not issue a lease.

The following is an example of a static binding configuration:

```
[edit system services dhcp]
static-binding 00:0d:56:f4:01:ab {
   fixed-address {
      10.5.5.5;
      10.6.6.6;
   }
   host-name "another-host.domain.tld";
   client-identifier hexadecimal 01001122aabbcc;
}
```

### Specifying DHCP Lease Times

For clients that do not request a specific lease time, the default lease time is one day. You can configure a maximum lease time for IP address assignments or change the default lease time.

To configure lease times, include the maximum-lease-time and default-lease-time statements:

```
maximum-lease-time;
default-lease-time;
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Lease times defined for static bindings and address pools take priority over lease times defined at the [edit system services dhcp] hierarchy level.

The maximum-lease-time statement configures the maximum length of time in seconds for which a client can request and hold a lease. If a client requests a lease longer than the maximum specified, the lease is granted only for the maximum time configured on the server. After a lease expires, the client must request a new lease.

**NOTE:** Maximum lease times do not apply to dynamic BOOTP leases. These leases are not specified by the client and can exceed the maximum lease time configured.

The following example shows a configuration for maximum and default lease times:

```
[edit system services dhcp]
maximum-lease-time 7200;
default-lease-time 3600;
```

### Configuring a Boot File and Boot Server

When a client starts, it contacts a boot server to download the boot file.

To configure a boot file and boot server, include the boot-file and boot-server statements:

```
boot-file filename;
boot-server address;
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

After a client receives a DHCPOFFER response from a DHCP server, the client can communicate directly with the boot server (instead of the DHCP server) to download the boot file. This minimizes network traffic and enables you to specify separate boot server/file pairs for each client pool or subnetwork.

The boot-file statement configures the name and location of the initial boot file that the DHCP client loads and executes. This file stores the boot image for the client. In most cases, the boot image is the operating system the client uses to load.

The boot-server statement configures the IP address of the TFTP server that contains the client's initial boot file. You must configure an IP address (not a hostname) for the server.

You must configure at least one boot file and boot server. Optionally, you can configure multiple boot files and boot servers. For example, you might configure two separate boot servers and files: one for static binding and one for address pools. Boot file configurations for pools or static bindings take precedence over boot file configurations at the [edit system services dhcp] hierarchy level.

The following example specifies a boot file and server for an address pool:

```
[edit system services dhcp]
pool 10.4.4.0/24 {
   boot-file "boot.client";
   boot-server 10.4.4.1;
}
```

### Configuring a DHCP Server Identifier

The host running the DHCP server itself must use a manually assigned, static IP address. It cannot send a request and receive an IP address from itself or another DHCP server.

To configure a server identifier, include the server-identifier statement:

```
server-identifier address;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The server-identifier statement specifies the IP address of the DHCP server. The host must be a TFTP server that is accessible by all clients served within a range of IP addresses (based on either an address pool or static binding).

The following example shows a DHCP server identifier configured for an address pool:

```
[edit system services dhcp]
pool 10.3.3.0/24 {
   address-range low 10.3.3.2 high 10.3.3.254;
   exclude-address {
      10.3.3.33;
   }
   router {
      10.3.3.1;
   }
   server-identifier 10.3.3.1;
}
```

### Configuring a Domain Name and Domain Search List

To configure the name of the domain in which clients will search for a DHCP server host, include the domain-name statement:

```
domain-name domain;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The domain-name statement sets the domain name that is appended to hostnames that are not fully qualified. This statement is optional. If you do not configure a domain name, the default is the client's current domain.

To configure a domain search list, include the domain-search statement:

```
domain-search [ domain-list ];
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The domain-search statement sets the order in which clients append domain names when searching for the IP address of a host. You can include one or more domain names in the list. For more information, see RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*.

The domain-search statement is optional, if you do not configure a domain search list, the default is the client's current domain.

### Configuring Routers Available to the Client

After a DHCP client loads the boot image and has booted, the client sends packets to a router.

To configure routers available to the client, include the router statement:

```
router {
   address;
}
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The router statement specifies a list of IP addresses for routers on the client's subnet. List routers in order of preference. You must configure at least one router for each client subnet.

The following example shows routers configured at the [edit system services dhcp] hierarchy level:

```
[edit system services dhcp]
router {
   10.6.6.1;
   10.7.7.1;
}
```

### Creating User-Defined DHCP

You can configure one or more user-defined options that are not included in the JUNOS default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

To configure a user-defined DHCP option, include the option statement:

```
option {
   [ (id-number option-type option-value) | (id-number array option-typeoption-value) ] ;
}
```

The option statement specifies the following values:

- *id-number*—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- *option-type*—Any of the following types: flag, byte, string, short, unsigned-short, integer, unsigned-integer, ip-address.
- array—An option can include an array of values.
- *option-value*—Value associated with an option. The option value must be compatible with the option type (for example, an On or Off value for a flag type).

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The following example shows user-defined DHCP options:

```
[edit system services dhcp]
option 19 flag off; # 19: "IP Forwarding" option
option 40 string "domain.tld"; # 40: "NIS Domain" option
option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
```

User-defined options that conflict with DHCP configuration statements are ignored by the server. For example, in the following configuration, the DHCP server ignores the user-defined option 3 router statement and uses the edit system services dhcp router statement instead:

```
[edit system services dhcp]
option 3 router 10.7.7.2; # 3: "Default Router" option
router {
   10.7.7.1;
}
```

### Example: Complete DHCP Server Configuration

This section shows a complete DHCP server configuration with address pools, static bindings, and user-defined options.

The following example shows statements at the [edit interfaces] hierarchy level. The interface's primary address (10.3.3.1/24) has a corresponding address pool (10.3.3.0/24) defined at the [edit system services] hierarchy level.

```
[edit interfaces]
fe-0/0/1 {
   unit 0 {
      family inet {
         address 10.3.3.1/24;
      }
   }
}
```

**NOTE:** You can configure a DHCP server only on an interface's primary IP address.

Statements at the [edit system services] hierarchy level include the following:

```
[edit system services]
dhcp {
   domain-name "domain.tld";
   maximum-lease-time 7200;
   default-lease-time 3600;
   name-server {
      10.6.6.6;
      10.6.6.7;
   }
   domain-search [ subnet1.domain.tld subnet2.domain.tld ];
   wins-server {
      10.7.7.7;
      10.7.7.9;
   }
   router {
      10.6.6.1;
      10.7.7.1;
   }
   option 19 flag off; # 19: "IP Forwarding" option
   option 40 string "domain.tld"; # 40: "NIS Domain" option
   option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
   pool 10.3.3.0/24 {
      address-range low 10.3.3.2 high 10.3.3.254;
      exclude-address {
         10.3.3.33;
      }
      router {
         10.3.3.1;
      }
      server-identifier 10.3.3.1;
   }
   pool 10.4.4.0/24 {
      boot-file "boot.client";
      boot-server 10.4.4.1;
   }
   static-binding 00:0d:56:f4:20:01 {
      fixed-address 10.4.4.4;
```

```
        host-name "host.domain.tld";
    }
    static-binding 00:0d:56:f4:01:ab {
        fixed-address {
            10.5.5.5;
            10.6.6.6;
        }
        host-name "another-host.domain.tld";
        client-identifier "01aa.001a.bc65.3e";
    }
}
```

### Example: Viewing DHCP Bindings

Use the CLI command show system services dhcp binding to view information about DHCP address bindings, lease times, and address conflicts.

The following example shows the binding type and lease expiration times for IP addresses configured on a router that supports a DHCP server:

```
user@host> show system services dhcp binding
IP Address       Hardware Address     Type    Lease expires at
192.168.1.2      00:a0:12:00:12:ab       static      never
192.168.1.3      00:a0:12:00:13:02       dynamic     2004-05-03 13:01:42 PDT
```

Enter an IP address to show binding for a specific IP address:

```
user@host> show system services dhcp binding 192.168.1.3
DHCP binding information:
IP address      192.168.1.3
Hardware address      00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30 aced-00:a0:12:00
3a 31 33 3a 30 32
Lease information:
Type       dynamic
Obtained at       2004-05-02 13:01:42 PDT
Expires at       2004-05-03 13:01:42 PDT
```

Use the detail option to show detailed binding information:

```
user@host> show system services dhcp binding detail
DHCP binding information:
IP address                 192.168.1.3
Hardware address           00:a0:12:00:12:ab
Pool                       192.168.1.0/24
Interface                  fe-0/0/0, relayed by 192.168.4.254
Lease information:
Type                       dynamic
Obtained at                2004-05-02 13:01:42 PDT
Expires at                 2004-05-03 13:01:42 PDT
DHCP options:
name-server foo.mydomain.tld
domain-name mydomain.tld
option 19 flag off
```

### Example: Viewing DHCP Address Pools

Use the CLI show system services dhcp pool command to view information about DHCP address pools.

The following example show address pools configured on a DHCP server:

```
user@ host> show system services dhcp pool
Pool name        Low address     High address     Excluded addresses
10.40.1.0/24     10.40.1.1       10.40.1.254      10.40.1.254
```

### Example: Viewing and Clearing DHCP Conflicts

When the DHCP server provides an IP address, the client performs an ARP check to make sure the address is not being used by another client and reports any conflicts back to the server. The server keeps track of addresses with conflicts and removes them from the address pool. Use the CLI command show system services dhcp conflict to show conflicts.

```
user@host> show system services dhcp conflict
Detection time                  Detection method       Address
2004-08-03 19:04:00 PDT         client      192.168.1.5
2004-08-04 04:23:12 PDT         ping      192.168.1.8
```

Use the clear system services dhcp conflicts command to clear the conflicts list and return IP addresses to the pool. The following command shows how to clear an address on the server that has a conflict:

```
user@host> clear system services dhcp conflict 192.168.1.5
```

**NOTE:** For more information about CLI commands you can use with the DHCP server, see the *JUNOS System Basics and Services Command Reference*.

### Tracing DHCP Processes

DHCP tracing operations track all DHCP operations and record them to a log file.

By default, no DHCP processes are traced. If you include the traceoptions statement at the [edit system services dhcp] hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called dhcpd located in the /var/log directory.
- When the file dhcpd reaches 128 kilobytes (KB), it is renamed dhcpd.0, then dhcpd.1, and so on, until there are 3 trace files. Then the oldest trace file (dhcpd.2 is overwritten). For more information about how log files are created, see the *JUNOS System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory in which trace files are located. However, you can customize the other trace file settings by including the following statements at the [edit system services dhcp traceoptions] hierarchy level.:

```
[edit system services dhcp traceoptions]
file filename <files number> <match regex> <size size> <world-readable |
   no-world-readable>;
flag {
   all;
}
```

These statements are described in the following sections:

- Configuring the DHCP Processes Log Filename on page 163
- Configuring the Number and Size of DHCP Processes Log Files on page 163
- Configuring Access to the Log File on page 164
- Configuring a Regular Expression for Line to Be Logged on page 164
- Configuring the Trace Operations on page 164

#### *Configuring the DHCP Processes Log Filename*

By default, the name of the file that records trace output is dhcpd. You can specify a different name by including the file statement at the [edit system services dhcp traceoptions] hierarchy level:

```
[edit system services dhcp traceoptions (DHCP Server on J-series Services Routers)]
file filename;
```

#### *Configuring the Number and Size of DHCP Processes Log Files*

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed *filename*.0, then *filename*.1, and so on, until there are 3 trace files. Then the oldest trace file (*filename*.2) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the [edit system services dhcp traceoptions] hierarchy level:

```
[edit system services dhcp traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (*filename*) reaches 2 MB, *filename* is renamed *filename*.0, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename*.0 is renamed *filename*.1 and *filename* is renamed *filename*.0. This process repeats until there are 20 trace files. Then the oldest file (*filename*.19) is overwritten by the newest file (*filename*.0).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

#### *Configuring Access to the Log File*

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the file world-readable statement at the [edit system services dhcp traceoptions] hierarchy level:

```
[edit system services dhcp traceoptions]
file world-readable;
```

To set the default behavior explicitly, include the file no-world-readable statement at the [edit system services dhcp traceoptions] hierarchy level:

```
[edit system services dhcp traceoptions]
file no-world readable;
```

#### *Configuring a Regular Expression for Line to Be Logged*

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the [edit system services dhcp traceoptions file *filename*] hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system services dhcp traceoptions]
file filename match regex;
```

#### *Configuring the Trace Operations*

By default, only important events are logged. You can configure the trace operations to be logged by including the following options at the [edit system services dhcp traceoptions] hierarchy level:

```
[edit dhcp system services dhcp traceoptions]
flag {
    all;
    binding;
    config;
    conflict;
    event;
    ifdb;
    io;
    lease;
    main;
    misc;
    packet;
    options;
    pool;
    protocol;
    rtsock;
    scope;
    signal;
    trace;
```

```
    ui;
}
```

Table 31 on page 165 describes which operation or event is recorded by each DHCP tracing flag. By default, all flags are disabled.

**Table 31: DHCP Processes Tracing Flags**

| Flag | Operation or Event |
|---|---|
| all | All operations. |
| binding | Binding operations. |
| config | Logins to the configuration database. |
| conflict | Client-detected conflicts for IP addresses. |
| event | Important events. |
| ifdb | Interface database operations. |
| io | I/O operations. |
| lease | Lease operations. |
| main | Main loop operations. |
| misc | Miscellaneous operations. |
| packet | DHCP packets. |
| options | DHCP options. |
| pool | Address pool operations. |
| protocol | Protocol operations. |
| rtsock | Routing socket operations. |
| scope | Scope operations. |
| signal | DHCP signal operations. |
| trace | Tracing operations. |
| ui | User interface operations. |

## *Configuring the Extended DHCP Local Server*

You can enable the router to function as an extended DHCP local server and configure the extended DHCP local server options on the router. The extended DHCP local server provides an IP address and other configuration information in response to a client request.

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See “Configuring Address-Assignment Pools” on page 457 for details about creating and using address-assignment pools.

**NOTE:** The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

You cannot configure the extended DHCP local server and extended DHCP relay on the same interface.

To configure the extended DHCP local server on the router, include the dhcp-local-server statement at the [edit system services] hierarchy level:

```
[edit system services]
dhcp-local-server {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    group group-name {
        authentication {
            password password-string;
```

```
            username-include {
               circuit-type;
               delimiter delimiter-character;
               domain-name domain-name-string;
               logical-system-name;
               mac-address;
               option-60;
               option-82 <circuit-id> <remote-id>;
               routing-instance-name;
               user-prefix user-prefix-string;
            }
         }
         interface interface-name <upto upto-interface-name> <exclude>;
      }
      pool-match-order {
         ip-address-first;
         option-82;
      }
      traceoptions {
         file filename <files number> <size size> <world-readable | no-world-readable>
            <match regex>;
         flag flag;
      }
   }
```

You can also include these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* system services]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services]
- [edit routing-instances *routing-instance-name* system services]

The following sections describe the operation and configuration of the extended DHCP local server and provide configuration examples:

**NOTE:** The extended DHCP local server is incompatible with the J-series DHCP server. As a result, the DHCP local server and the DHCP/BOOTP relay agent cannot both be enabled on the router at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

### Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the router. The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.
2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.
3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server that will grant the address and configuration information.
4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

### Using Address Assignment Pools

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by

the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See “Configuring Address-Assignment Pools” on page 457 for details about creating and using address-assignment pools.

**NOTE:** The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

## Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use

You can specify the method that the extended DHCP local server uses to determine which address-assignment pool provides the IP address and configuration for a DHCP client. By default, the server matches the IP address in the client DHCP request to the address of the address-assignment pool.

### *Matching Client IP Address to Address-Assignment Pool*

In the default configuration, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool’s address. If there is no giaddr in the request, the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

### *Matching Option 82 Information to Named Address Ranges*

You can also configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, and are configured when you create the address-assignment pool. To use the DHCP local server option 82 matching feature, you must ensure that the option-82 statement is included in the dhcp-attributes statement for the address-assignment pool.

**NOTE:** To enable the option 82 matching method, you must first specify the ip-address-first statement in the pool-match-order statement, and then specify the option-82 statement.

### Using Default Options

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- router—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
- domain name—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
- domain name server—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

### Using External AAA Authentication Services

Both the extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.

**NOTE:** This section uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the authentication-server statement at the [edit access profile *profile-name*] hierarchy level.

To configure authentication support for an extended DHCP application, include the authentication statement at these hierarchy levels. You can configure either global authentication support or group-specific support.

You must configure the username-include statement to enable the use of authentication. The password statement is not required and does not cause DHCP to use authentication if the username-include statement is not included.

Extended DHCP local server hierarchies:

- [edit system services dhcp-local-server]
- [edit system services dhcp-local-server group *group-name*]

- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]
- [edit routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]

Extended DHCP relay agent hierarchies:

- [edit forwarding-options dhcp-relay]
- [edit forwarding-options dhcp-relay group *group-name*]
- [edit logical-systems *logical-system-name* forwarding-options dhcp-relay]
- [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]
- [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]
- [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]

```
authentication {
   password password-string;
   username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
   }
}
```

### *Grouping Interfaces with Common DHCP Configurations*

The extended DHCP applications enable you to group together a set of interfaces and apply a common DHCP configuration to the named interface group.

To configure an interface group, use the group statement.

```
group group-name {
   authentication {
      password password-string;
      username-include {
         circuit-type;
         delimiter delimiter-character;
         domain-name domain-name-string;
         logical-system-name;
         mac-address;
         option-60;
         option-82 <circuit-id> <remote-id>;
         routing-instance-name;
         user-prefix user-prefix-string;
      }
   }
   interface interface-name <upto upto-interface-name> <exclude>;
}
```

You can specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the interface *interface-name* statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. For example:

```
group boston {
   interface 192.168.10.1;
   interface 192.168.15.5;
}
```

You can use the *upto* option to specify a range of interfaces on which the extended DHCP application is enabled. For example:

```
group quebec {
   interface 192.168.10.1 upto 192.168.10.255;
}
```

You can use the exclude option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
group paris {
   interface 192.168.100.1 exclude;
   interface 192.168.100.100 upto 192.168.100.125 exclude;
}
```

### *Configuring Passwords for Usernames*

You can configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

To configure a password that authenticates the username, use the password statement. See “Configuring Special Requirements for Plain-Text Passwords” on page 55 for information about supported characters in passwords. For example:

```
authentication {
   password myPassworD1234
}
```

### *Creating Unique Usernames*

You can configure the extended DHCP application to include additional fields in the username passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers.

**NOTE:** No authentication is performed if you do not include a username in the authentication configuration; however, the IP address is provided by the local pool if it is configured.

To configure unique usernames, use the username-include statement. You can include any or all of the additional statements.

```
authentication {
   username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
   }
}
```

The following list describes the attributes that can be included as part of the username:

- circuit-type—The circuit type used by the DHCP client, for example enet.
- delimiter—The delimiter character that separates components that make up the concatenated username. The semicolon (;) is not supported as a delimiter character.
- domain-name—The client domain name as string. The router adds the @ delimiter to the username.
- logical-system-name—The name of the logical system, if the receiving interface is in a logical system.
- mac-address—The client MAC address, in a string of the format *xxxx.xxxx.xxxx*.
- option-60—The portion of the option 60 payload that follows the length field.

- option-82 <circuit-id> <remote-id>;—The specified contents of the option 82 payload.
  - circuit-id—The payload of the Agent Circuit ID suboption.
  - remote-id—The payload of the Agent Remote ID suboption.
  - Both circuit-id and remote-id—The payloads of both suboptions, in the format: circuit-id[delimiter]remote-id.
  - Neither circuit-id or remote-id—The raw payload of the option 82 from the PDU is concatenated to the username.
- routing-instance-name—The name of the routing instance, if the receiving interface is in a routing instance.
- user-prefix—A string indicating the user prefix.

The router creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter. The default delimiter is a period (.). You can specify a different delimiter; however, the semicolon character (;) is not allowed.

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]
routing-instance-name[delimiter]circuit-type[delimiter]option-82[delimiter]
option-60@domain-name
```

#### *Example: Configuring a Unique Username*

This example shows a sample configuration that creates a unique username. The username is shown after the configuration.

**Configuration**

```
authentication {
   username-include {
      circuit-type;
      domain-name isp55.com;
      mac-address;
      user-prefix wallybrown;
   }
}
```

**Resulting Unique Username**

wallybrown.0090.1a01.1234.enet@isp55.com

#### *Providing Client Configuration Information*

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool, the extended DHCP application

merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional — a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address assignment pool to provide the configuration for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. The following list shows the information that RADIUS might include in the authentication grant. See "RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework" on page 451 for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management.

- Client IP address—RADIUS attribute 8, Framed-IP-Address
- Subnet mask for client IP address (DHCP option 1)—RADIUS attribute 9, Framed-IP-Netmask
- Primary domain server (DHCP option 6)—VSA 26-4, Primary-DNS
- Secondary domain server (DHCP option 6)—VSA 26-5 Secondary-DNS
- Primary WINS server (DHCP option 44)—VSA 26-6, Primary-WINS
- Secondary WINS server (DHCP option 44)—VSA 26-7, Secondary-WINS
- Address assignment pool name—RADIUS attribute 88, Framed-Pool
- Lease time—RADIUS attribute 27, Session-Timeout
- DHCP relay server—VSA 26-109, DHCP-Guided-Relay-Server

### Tracing Extended DHCP Local Server Operations

The extended DHCP tracing operations track the extended DHCP local server operations and record them in a log file. By default, no extended DHCP local server processes are traced. If you include the traceoptions statement at the [edit system services dhcp-local-server] hierarchy level, the default tracing behavior is the following:

- Important extended DHCP local server events are logged in a file called jdhcpd located in the /var/log directory.
- When the file jdhcpd reaches 128 kilobytes (KB), it is renamed jdhcpd.0, then jdhcpd.1, and so on, until there are 3 trace files. Then the oldest trace file (jdhcpd.2) is overwritten. For more information about how log files are created, see the *JUNOS System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.

To trace DHCP local server operations, include the traceoptions statement at the [edit system services dhcp-local-server] hierarchy level:

```
traceoptions {
   file filename <files number> <size size> <world-readable | no-world-readable> <match
      regex>;
   flag flag;
}
```

#### Configuring the Extended DHCP Local Server Processes Log Filename

By default, the name of the file that records trace output is jdhcpd. You can specify a different name by including the file statement at the [edit system services dhcp-local-server traceoptions] hierarchy level:

```
[edit system services dhcp-local-server traceoptions]
file filename;
```

#### Configuring the Number and Size of Extended DHCP Local Server Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed jdhcpd.0, then jdhcpd.1, and so on, until there are three trace files. Then the oldest trace file (jdhcpd.2) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the [edit system services dhcp-local-server traceoptions] hierarchy level:

```
[edit system services dhcp-local-server traceoptions]
file filename files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (jdhcpd) reaches 2 MB, jdhcpd is renamed jdhcpd.0, and a new file called jdhcpd is created. When the new jdhcpd reaches 2 MB, jdhcpd.0 is renamed jdhcpd.1 and *filename* is renamed jdhcpd.0. This process repeats until there are 20 trace files. Then the oldest file (jdhcpd.19) is overwritten by the newest file (jdhcpd.0).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

#### Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the file world-readable statement at the [edit system services dhcp-local-server traceoptions] hierarchy level:

```
[edit system services dhcp-local-server traceoptions]
file filename world-readable;
```

To set the default behavior explicitly, include the file no-world-readable statement at the [edit system services dhcp-local-server traceoptions] hierarchy level:

```
[edit system services dhcp-local-server traceoptions]
file filename no-world readable;
```

#### *Configuring a Regular Expression for Line to Be Logged*

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the [edit system services dhcp-local-server traceoptions] hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system services dhcp-local-server traceoptions]
file filename match regex;
```

#### *Configuring Trace Option Flags*

By default, only important events are logged. You can configure the trace operations to be logged by including extended DHCP local server tracing flags at the [edit system services dhcp-local-server traceoptions] hierarchy level:

```
[edit system services dhcp-local-server traceoptions]
flag flag;
```

You can configure the following tracing flags:

- all—Trace all operations.
- auth—Trace authentication operations.
- database—Trace database events.
- fwd—Trace firewall process events.
- general—Trace miscellaneous events.
- ha—Trace high availability-related events.
- interface—Trace interface operations.
- io—Trace I/O operations.
- packet—Trace packet decoding operations.
- packet-option—Trace DHCP option decoding operations.
- rpd—Trace routing protocol process events.
- rtsock—Trace routing socket operations.
- session-db—Trace session database operations.
- state—Trace changes in state.
- ui—Trace user interface operations.

### Example: Minimum Extended DHCP Local Server Configuration

The following example shows the minimum configuration you need to use the extended DHCP local server on the router:

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
    }
}
```

This example creates the server group named group_one, and specifies that the DHCP local server is enabled on interface fe-0/0/2.0 within the group. The DHCP local server uses the default pool match configuration of ip-address-first.

### Example: Extended DHCP Local Server Configuration with Optional Pool Matching

The following example shows an extended DHCP local server configuration that includes optional pool matching and interface groups. This configuration specifies that the DHCP local server uses option 82 information to match the named address range for client IP address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
        interface fe-0/0/2.1;
    }
    group group_two {
        interface fe-0/0/3.0;
        interface fe-0/0/3.1;
    }
    pool-match-order {
        ip-address-first:
        option-82:
    }
}
```

### Verifying and Managing DHCP Local Server Configuration

To display the client address bindings for the extended DHCP local server, use the following operational commands:

- show dhcp server binding
- show dhcp server statistics

To clear client address bindings and DHCP local server statistics, use the following operational commands:

- clear dhcp server binding
- clear dhcp server statistics

For information about using these operations commands, see the *JUNOS System Basics and Services Reference*.

### *Configuring DTCP-over-SSH Service for the Flow-Tap Application*

The active monitoring flow-tap application requires you to configure the flow-tap DTCP-over-SSH service. Flow-tap enables you to intercept IPv4 packets transiting an active monitoring router and send a copy of matching packets to one or more content destinations, for use in flexible trend analysis of security threats and in lawful intercept of data.

To enable the flow-tap DTCP-over-SSH service, include the following statements at the [edit system services] hierarchy level:

```
flow-tap-dtcp {
    ssh {
        <connection-limit limit>;
        <rate-limit limit>;
    }
}
```

By default, the router supports a limited number of simultaneous flow-tap DTCP-over-SSH sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- connection-limit *limit*—Maximum number of simultaneous connections (a value from 1 through 250). The default is 75.
- rate-limit *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.

You must also define user permissions that enable flow-tap users to configure flow-tap services. Specify a login class and access privileges for flow-tap users at the [edit system login class *class-name* permissions] hierarchy level:

```
[edit system login class class-name permissions]
(flow-tap | flow-tap-control | flow-tap-operation);
```

The permission bit for a flow-tap login class can be one of the following:

- flow-tap—Can view the flow-tap configuration in configuration mode.
- flow-tap-control—Can view the flow-tap configuration in configuration mode and configure flow-tap configuration information at the [edit services flow-tap] hierarchy level.
- flow-tap-operation—Can make flow-tap requests to the router from a remote location using a DTCP client.

**NOTE:** Only users with a configured access privilege of flow-tap-operation can initiate flow-tap requests.

For more information about how to define login classes, see “Defining Login Classes” on page 61.

You can also specify user permissions through the Juniper-User-Permissions RADIUS attribute. For more information, see “Configuring Juniper Networks Vendor-Specific RADIUS Attributes” on page 78.

To enable the flow-tap DTCP-over-SSH service, you must also include statements at the [edit interfaces] hierarchy level to specify an Adaptive Services PIC that runs the flow-tap service and conveys flow-tap filters from the mediation device to the router. In addition, you must include the flow-tap statement at the [edit services] hierarchy level. For more information, see the *JUNOS Services Interfaces Configuration Guide*.

## Configuring Finger Service

To configure the router to accept finger as an access service, include the finger statement at the [edit system services] hierarchy level:

```
[edit system services]
finger {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

By default, the router supports a limited number of simultaneous finger sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- connection-limit *limit*—Maximum number of simultaneous connections (a value from 1 through 250). The default is 75.
- rate-limit *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.

You cannot include the finger statement on routers that run the JUNOS-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

## Configuring FTP Service

To configure the router to accept FTP as an access service, include the ftp statement at the [edit system services] hierarchy level:

```
[edit system services]
ftp {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

By default, the router supports a limited number of simultaneous FTP sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- connection-limit *limit*—Maximum number of simultaneous connections (a value from 1 through 250). The default is 75.

- rate-limit *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.

You can use passive FTP to access devices that accept only passive FTP services. All commands and statements that use FTP also accept passive FTP. Include the ftp statement at the [edit system services] hierarchy level to use either active FTP or passive FTP.

To start a passive FTP session, use pasvftp (instead of ftp ) in the standard FTP format (ftp://*destination*). For example:

```
request system software add pasvftp://name.com/jinstall.tgz
```

You cannot include the ftp statement on routers that run the JUNOS-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

## *Configuring SSH Service*

To configure the router to accept SSH as an access service, include the ssh statement at the [edit system services] hierarchy level:

```
[edit system services]
ssh {
   root-login (allow | deny | deny-password);
   protocol-version [v1 v2];
   <connection-limit limit>;
   <rate-limit limit>;
}
```

By default, the router supports a limited number of simultaneous SSH sessions and connection attempts per minute. For information about system process limits see “Process Limits” on page 10. Optionally, you can include either or both of the following statements to change the defaults:

- connection-limit *limit*—Maximum number of simultaneous connections (a value from 1 through 250). The default is 75.
- rate-limit *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.

For information about other configuration settings, see the following sections:


- Configuring the Root Login on page 181
- Configuring the SSH Protocol Version on page 182


### Configuring the Root Login

By default, users are allowed to log in to the router as root through SSH. To control user access through SSH, include the root-login statement at the [edit systems services ssh] hierarchy level:

```
[edit system services ssh]
```

```
root-login (allow | deny | deny-password);
```

allow—Allows users to log in to the router as root through SSH. The default is allow.

deny—Disables users from logging in to the router as root through SSH.

deny-password—Allows users to log in to the router as root through SSH when the authentication method (for example, RSA) does not require a password.

**NOTE:** The root-login and protocol-version statements are supported in JUNOS Release 5.0 and later. If you downgrade to a release prior to Release 5.0, the root-login and protocol-version statements are ignored if they are present in the configuration file.

#### Configuring the SSH Protocol Version

By default, version 2 of the SSH protocol is enabled. To configure the router to use only version 1of the SSH protocol, include the protocol-version statement and specify v1 at the [edit system services ssh] hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 ];
```

To configure the router to use version 1 and 2 of the SSH protocol, include the protocol-version statement and specify v1 and v2 at the [edit system services ssh] hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 v2 ];
```

You can specify v1, v2, or both versions ([ v1 v2 ]) of the SSH protocol. The default is v2.

For J-series Services Routers, the export license software only supports SSH version 1.

**NOTE:** The root-login and protocol-version statements are supported in JUNOS Release 5.0 and later. If you downgrade to a release prior to release 5.0, the root-login and protocol-version statements are ignored if they are present in the configuration file.

### *Configuring Outbound SSH Service*

You can configure a router running the JUNOS software to initiate a TCP/IP connection with a client management application that would be blocked if the client attempted to initiate the connection (for example, if the router is behind a firewall). A single outbound-ssh configuration statement instructs the router to create a TCP/IP connection with the client management application and to forward the router's identity. Once the connection is established, the management application initiates the SSH sequence as the client and the router as the server that authenticates the client.

**NOTE:** There is no initiation command with outbound SSH. Once outbound SSH is configured and committed, the router begins to initiate an outbound SSH connection based on the committed configuration. It continues to attempt to create this connection until successful. If the connection between the router and the client management application is broken, the router again attempts to create a new outbound SSH connection until successful. This connection is maintained until the outbound SSH stanza is removed from the configuration.

To configure the router running JUNOS software for outbound SSH connections, include the outbound-ssh statement at the [edit system services] hierarchy level:

```
[edit system services]
outbound-ssh {
   client client-id {
      address {
         port port-number;
         retry number;
         timeout seconds;
      }
      device-id device-id;
      keep-alive {
         retry number;
         timeout seconds;
      }
      reconnect-strategy (in-order | sticky);
      secret password;
      services netconf;
   }
   traceoptions {
      file filename <files number> <match regex> <size size> <world-readable |
         no-world-readable>;
      flag flag;
      no-remote-trace;
   }
}
```



### Understanding the Client

The client *client-id* value is not forwarded to the client management application. This value serves to uniquely identify the outbound-ssh configuration stanza. Each

outbound-ssh stanza represents a single outbound SSH connection. Thus, the administrator is free to assign the client-id any meaningful unique value.

### Identifying the Device to the Client

Each time the router establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router to the management client. Within this transmission is the value of *device-id*.

To configure the router's device identifier, include the device-id statement at the [edit system services outbound-ssh client *client-id*] hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when secret is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

### Sending the Router's Public SSH Key

During the initialization of an SSH connection, the client authenticates the identity of the router using the router's public SSH host key. Therefore, before the client can initiate the SSH sequence, it needs the router's public SSH key. When you configure the secret statement, the router running JUNOS software passes the router's public SSH key as part of the outbound SSH connection initiation sequence.

When the secret statement is set and the router establishes an outbound SSH connection, the router communicates its device ID, its public SSH key, and an SHA1 hash derived in part from the secret statement. The value of the secret statement is shared between the router and the management client. The client uses the shared secret to authenticate the public SSH host key it is receiving to determine whether the public key is from the router identified by the device-id statement.

Using the secret statement to transport the router's public SSH host key is optional. You can manually transport and install the public key onto the client system.

**NOTE:** Including the secret statement means that the router's public SSH host key is sent every time the router establishes a connection to the client. It is then up to the client to decide what to do with the SSH host key if it already has one for that router. We recommend that you replace the client's copy with the new key. Host keys can change for various reasons and by replacing the key each time a connection is established, you ensure that the client has the latest key.

To configure a router that is running the JUNOS software to send the router's public SSH host key when connection to the client occurs, include the secret statement at the [edit system services outbound-ssh client *client-id*] hierarchy level:

```
[edit system services outbound-ssh client client-id]
```

```
secret password;
```

The message sent by the JUNOS router when the secret attribute is configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
HOST-KEY: <public-hot-key>\r\n
HMAC:<HMAC(pub-SSH-host-key, <secret>>)>\r\n
```

### Using the Standard SSH Sequence

Once the client application has the router's public SSH host key, it can then initiate the SSH sequence as if it had created the TCP/IP connection and authenticate the router using its copy of the router's public host SSH key as part of that sequence. The router authenticates the client user through the mechanisms supported in the JUNOS software (RSA/DSA public string or password authentication).

### Configuring Keepalive Messages

To enable the router to send SSH protocol keepalive messages to the client application, configure the keep-alive statement at the [edit system services outbound-ssh client *client-id*] hierarchy level:

```
[edit system services outbound-ssh client client-id]
keep-alive {
    retry number;
    timeout seconds;
}
```

The timeout option specifies how long the router waits to receive data before sending a request for acknowledgment from the application. The default is 15 seconds.

The retry option specifies how many keepalive messages the router sends without receiving a response from the client. When that number is exceeded, the router disconnects from the application, ending the outbound SSH connection. The default is three retries.

### Configuring the reconnect-strategy Statement

When disconnected, the router begins to initiate a new outbound SSH connection. To specify how the router reconnects to the server after a connection is dropped, include the reconnect-strategy statement at the [edit system services outbound-ssh client *client-id*] hierarchy level:

```
[edit system services outbound-ssh client-id]
reconnect-strategy (sticky | in-order);
```

The sticky option configures the router to reconnect to the server that it disconnected.

The in-order option configures the router to reconnect to the first configured server. If this server is unavailable, the router tries to connect to the next configured server. This process repeats until a connection is completed.

You can also specify the number of retry attempts and set the amount of time before stopping the reconnection attempts. See “Configuring Keepalive Messages” on page 185.

### Configuring the services Statement

To configure the application to accept NETCONF as an available service, include the services netconf statement at the [edit system services outbound-ssh client *client-id*] hierarchy level:

```
[edit system services outbound-ssh client client-id]
services {
    netconf;
}
```

### Configuring Outbound SSH Clients

To configure the clients available for this outbound SSH connection, list each client with a separate address statement at the [edit system services outbound-ssh client *client-id*] hierarchy level:

```
[edit system services outbound-ssh client client-id]
    address {
        retry number;
        timeout seconds;
        port port-number;
    }
```

The address statement is the IP address or host name of the client.

The timeout statement specifies how long the application waits between attempts to reconnect to the specified IP address, in seconds. The default is 15 seconds.

The retry statement specifies how many connection attempts a router can make to to the specified IP address. The default is 3.

The port statement specifies the port at which a server listens for outbound SSH connection requests.

## *Configuring Telnet Service*

To configure the router to accept Telnet as an access service, include the telnet statement at the [edit system services] hierarchy level:

```
[edit system services]
telnet {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

By default, the router supports a limited number of simultaneous Telnet sessions and connection attempts per minute.

Optionally, you can include either or both of the following statements to change the defaults:

- connection-limit *limit*—Maximum number of simultaneous connections (a value from 1 through 250). The default is 75.
- rate-limit *limit*—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150.

You cannot include the telnet statement on routers that run the JUNOS-FIPS software. We recommend that you do not use Telnet in a Common Criteria environment.

## Configuring Console Access to PICs

By default, there is no password setting for console access. To configure console access to the Physical Interface Cards (PICs), include the pic-console-authentication statement at the [edit system] hierarchy level:

```
[edit system]
pic-console-authentication {
   (encrypted-password "password" | plain-text-password);
}
```

encrypted-password "*password*"—Use Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

plain-text-password—Use a plain-text password. The command-line interface (CLI) prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.

## Configuring a System Login Message

By default, no login message is displayed. To configure a system login message, include the message statement at the [edit system login] hierarchy level:

```
[edit system login]
message text;
```

If the message text contains any spaces, enclose it in quotation marks.

Special Characters—You can format the message using the following special characters:

- \n—New line
- \t—Horizontal tab
- \'—Single quotation mark

- \"—Double quotation mark
- \\—Backslash

**Example of a Login Message Configuration**

```
[edit]
system {
    login {
        message "\n\n\n\tUNAUTHORIZED USE OF THIS SYSTEM\n
                 \tIS STRICTLY PROHIBITED!\n\n\tPlease contact
                 \'company-noc@company.com\' to gain\naccess
                 to this equipment if you need authorization.\n\n\n";
        }
    }
}
```

The above login message configuration example would produce a login message similar to the following:

```
server% telnet router1
Trying 1.1.1.1...
Connected to router1.
Escape character is '^]'.


          UNAUTHORIZED USE OF THIS SYSTEM
          IS STRICTLY PROHIBITED!

          Please contact 'company-noc@company.com' to gain
          access to this equipment if you need authorization.



router1 (ttyp0)

login:
```

A system login message appears before the user logs in. A system login announcement appears after the user logs in. See “Configuring a System Login Announcement” on page 188.

## Configuring a System Login Announcement

By default, no login announcement is displayed. To configure a system login announcement, include the announcement statement at the [edit system login] hierarchy level:

```
[edit system login]
announcement text;
```

If the announcement text contains any spaces, enclose it in quotation marks.

A system login announcement appears after the user logs in. A system login message appears before the user logs in. See “Configuring a System Login Message” on page 187.

**TIP:** You can use the same special characters described in "Configuring a System Login Message" on page 187 to format your system login announcement.

## Configuring JUNOS Software Processes

By default, all JUNOS software processes are enabled on the router. To control the software processes on the router, you can do the following:

- Disabling JUNOS Software Processes on page 189
- Configuring Failover to Backup Media if a Software Process Fails on page 189

### *Disabling JUNOS Software Processes*

**CAUTION:** Never disable any of the software processes unless instructed to do so by a Customer Support engineer.

To disable a software process, specify the appropriate option in the processes statement at the [edit system] hierarchy level:

```
[edit system]
processes {
   process-name (enable | disable);
}
```

**NOTE:** The *process-name* variable is one of the valid process names. You can obtain a complete list of process names by using the CLI command completion feature. For additional information, see processes.

### *Configuring Failover to Backup Media if a Software Process Fails*

For routers with redundant Routing Engines, you can configure the routing platform to switch to backup media that contains a version of the system if a software process fails repeatedly. You can configure the routing platform to fail over either to backup media or to the other Routing Engine. To configure automatic switchover to backup media if a software process fails, include the failover statement at the [edit system processes *process-name*] hierarchy level:

```
[edit system processes]
process-name failover (alternate-media | other-routing-engine);
```

*process-name* is one of the valid process names. If this statement is configured for a process, and that process fails four times within 30 seconds, the router reboots from either the alternative media or the other Routing Engine. For more information about the boot sequence, see the *JUNOS Software Installation and Upgrade Guide*.

## Configuring the Password on the Diagnostics Port

If you have been asked by Customer Support personnel to connect a physical console to a control board or forwarding component on the router (such as the System Control Board [SCB], System and Switch Board [SSB], or Switching and Forwarding Module [SFM]) to perform diagnostics, you can configure a password on the diagnostics port. This password provides an extra level of security.

To configure a password on the diagnostics port, include the diag-port-authentication statement at the [edit system] hierarchy level:

```
[edit system]
diag-port-authentication (encrypted-password "password" | plain-text-password);
```

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

You can use an MD5 password, or you can enter a plain-text password that the JUNOS software encrypts (using MD5-style encryption) before it places it into the password database. For an MD5 password, specify the password in the configuration. Null-password (empty) is not permitted.

If you configure the plain-text-password option, the CLI prompts you for the password.

For routers that have more than one SSB, the same password is used for both SSBs.

## Viewing Core Files from JUNOS Processes

When an internal JUNOS process generates a core file, the output found at /var/crash/ and /var/tmp/ can now be viewed. This provides a quick method of finding core issues across large networks.

Use the CLI command show system core-dumps to view core dumps.

```
root@host> show system core-dumps
-rw-------  1 root  wheel  268369920 Jun 18 17:59 /var/crash/vmcore.0
-rw-rw----  1 root  field    3371008 Jun 18 17:53 /var/tmp/rpd.core.0
-rw-r--r--  1 root  wheel   27775914 Jun 18 17:59 /var/crash/kernel.0
```

## Saving Core Files from JUNOS Processes

By default, when an internal JUNOS process generates a core file, the file and associated context information are saved for debugging purposes in a compressed tar file named /var/tmp/*process-name*.core.*core-number*.tgz. The contextual information includes the configuration and system log message files.

To disable the saving of core files and associated context information, include the no-saved-core-context statement at the [edit system] hierarchy level:

```
[edit system]
no-saved-core-context;
```

To save the core files only, include the saved-core-files statement at the [edit system] hierarchy level and specify the number of files to save:

```
[edit system]
saved-core-files number;
```

*number* is the number of core files to save and can be a value from 1 through 64.

To save the core files along with the contextual information, include the saved-core-context statement at the [edit system] hierarchy level:

```
[edit system]
saved-core-context;
```

## Configuring Logical System Administrators

Using the JUNOS software, you can partition a single router into multiple logical devices that perform independent routing tasks. When creating logical systems, you must configure logical system administrators and interfaces, assign logical interfaces to logical systems, and configure various other logical system statements.

**NOTE:** In JUNOS Release 9.3 and later, the term *logical system* replaces the term *logical router*.

All configuration statements, operational commands, show command outputs, error messages, log messages, and SNMP MIB objects that contain the string logical-router or logical-routers have been changed to logical-system and logical-systems, respectively.

The master administrator can assign one or more logical system administrators to each logical system. Once assigned to a logical system, administrators are restricted to viewing only configurations of the logical system to which they are assigned and accessing only the operational commands that apply to that particular logical system. This restriction means that these administrators cannot access global configuration statements, and all command output is restricted to the logical system to which the administrators are assigned.

To configure logical system administrators, include the logical-system *logical-system-name* statement at the [edit system login class *class-name*] hierarchy level and apply the class to the user. For example:

```
[edit]
system {
   login {
      class admin1 {
         permissions all;
         logical-system logical-system-LS1;
      }
      class admin2 {
         permissions view; # Gives users assigned to class admin2 the ability to view
            # but not to change the configuration.
```

```
            logical-system logical-system-LS2;
        }
        user user1 {
            class admin1;
        }
        user user2 {
            class admin2;
        }
    }
}
```

Fully implementing logical systems requires that you also configure any protocols, routing statements, and policy statements for the logical system. For detailed information about implementing logical systems, see the *JUNOS Feature Guide* and the *JUNOS Routing Protocols Configuration Guide*.

## Configuring a Router to Transfer Its Configuration to an Archive Site

If you want to back up your router's current configuration to an archive site, you can configure the router to transfer its currently active configuration by FTP periodically or after each commit.

To configure the router to transfer its currently active configuration to an archive site, include statements at the [edit system archival configuration] hierarchy level:

```
[edit system archival configuration]
transfer-interval interval;
transfer-on-commit;
archive-sites {
    ftp://username<:password>@host-address<:port>/url-path;
    scp://username<:password>@host-address<:port>/url-path;
}
```

**NOTE:** When specifying a URL in a JUNOS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example,
"ftp://*username*<:*password*>@[*ipv6-host-address*]<:*port*>/*url-path*"

This section includes the following topics:



### Configuring the Transfer Interval

To configure the router to periodically transfer its currently active configuration to an archive site, include the transfer-interval statement at the [edit system archival configuration] hierarchy level:

```
[edit system archival configuration]
```

transfer-interval *interval*;

The *interval* is a period of time ranging from 15 through 2880 minutes.

### Configuring Transfer on a Commit Operation

To configure the router to transfer its currently active configuration to an archive site each time you commit a candidate configuration, include the transfer-on-commit statement at the [edit system archival configuration] hierarchy level:

```
[edit system archival configuration]
transfer-on-commit;
```

**NOTE:** When specifying a URL in a JUNOS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example,
"scp://*username*<:*password*>@[*ipv6-host-address*]<:*port*>/*url-path*"

### Configuring Archive Sites for Configuration Files

When you configure the router to transfer its configuration files, you specify an archive site to which the files are transferred. If you specify more than one archive site, the router attempts to transfer files to the first archive site in the list, moving to the next site only if the transfer fails.

When you use the archive-sites statement, you can specify a destination as a Hypertext Transfer Protocol (HTTP) URL, FTP URL, or secure copy (SCP)-style remote file specification. The URL type file:// is also supported.

To configure the archive site, include the archive-sites statement at the [edit system archival configuration] hierarchy level:

```
[edit system archival configuration]
archive-sites {
    ftp://username@host:<port>url-path password password;
    http://username@host:<port>url-path password password;
    scp://username@host:<port>url-path password password;
    file://<path>/<filename>;
}
```

**NOTE:** When specifying a URL in a JUNOS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example,
"scp://*username*<:*password*>@[*ipv6-host-address*]<:*port*>/*url-path*"

When you specify the archive site, do not add a forward slash (/) to the end of the URL. The format for the destination filename is as follows:

<*router-name*>_juniper.conf[.gz]_*YYYYMMDD_HHMMSS*

**NOTE:** The time included in the destination filename is always in Coordinated Universal Time (UTC) regardless of whether the time on the router is configured as UTC or the local time zone. The default time zone on the router is UTC.

## Specifying the Number of Configurations Stored on the CompactFlash Card

By default, the JUNOS software saves the current configuration and three previous versions of the committed configuration on the CompactFlash card. The currently operational JUNOS software configuration is stored in the file juniper.conf.gz, and the last three committed configurations are stored in the files juniper.conf.1.gz, juniper.conf.2.gz, and juniper.conf.3.gz. These four files are located in the router's CompactFlash card in the directory /config.

In addition to saving the current configuration and the current operational version, you can also specify how many previous versions of the committed configurations you want stored on the CompactFlash card in the directory /config. The remaining previous versions of committed configurations are stored in the directory /var/db/config on the hard disk. This is useful when you have very large configurations that might not fit on the CompactFlash card.

To specify how many previous versions of the committed configurations you want stored on the CompactFlash card, include the max-configurations-on-flash statement at the [edit system] hierarchy level:

```
[edit system]
max-configurations-on-flash number;
```

*number* is a value from 0 through 49.

## Configuring RADIUS System Accounting

With RADIUS accounting enabled, Juniper Network routers, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. The framework for RADIUS accounting is described in RFC 2866.

To audit user events, include the following statements at the [edit system accounting] hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
    radius {
        server {
            server-address {
                accounting-port port-number;
                secret password;
                source-address address;
                retry number;
                timeout seconds;
```

```
        }
      }
    }
  }
```

This section includes the following topics:



### *Specifying Events*

To specify the events you want to audit, include the **events** statement at the [edit system accounting] hierarchy level:

```
[edit system accounting]
events [ events ];
```

*events* is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

### *Configuring RADIUS Accounting*

To configure RADIUS server accounting, include the **server** statement at the [edit system accounting destination radius] hierarchy level:

```
server {
   server-address {
      accounting-port port-number;
      secret password;
      source-address address;
      retry number;
      timeout seconds;
   }
}
```

*server-address* specifies the address of the RADIUS server. To configure multiple RADIUS servers, include multiple **server** statements.

**NOTE:** If no RADIUS servers are configured at the [edit system accounting destination radius] statement hierarchy level, the JUNOS software uses the RADIUS servers configured at the [edit system radius-server] hierarchy level.

accounting-port *port-number* specifies the RADIUS server accounting port number.

The default port number is 1813.

**NOTE:** If you enable RADIUS accounting at the [edit access profile *profile-name* accounting-order] hierarchy level, accounting is triggered on the default port of 1813 even if you do not specify a value for the accounting-port statement.

You must specify a secret (password) that the local router passes to the RADIUS client by including the secret statement. If the password contains spaces, enclose the entire password in quotation marks (“ ”).

In the source-address statement, specify a source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router interfaces.

Optionally, you can specify the number of times that the router attempts to contact a RADIUS authentication server by including the retry statement. By default, the router retries three times. You can configure the router to retry from 1 through 10 times.

Optionally, you can specify the length of time that the local router waits to receive a response from a RADIUS server by including the timeout statement. By default, the router waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

### *Example: Configuring RADIUS Accounting*

The following example shows three servers (10.5.5.5, 10.6.6.6, and 10.7.7.7) configured for RADIUS accounting.

```
system {
   accounting {
      events [ login change-log interactive-commands ];
      destination {
         radius {
            server {
               10.5.5.5 {
                  accounting-port 3333;
                  secret $9$dkafeqwrew;
                  source-address 10.1.1.1;
                  retry 3;
                  timeout 3;
               }
               10.6.6.6 secret $9$fe3erqwrez;
               10.7.7.7 secret $9$f34929ftby;
            }
         }
      }
   }
}
```

## Configuring TACACS+ System Accounting

You can use TACACS+ to track and log software logins, configuration changes, and interactive commands. To audit these events, include the following statements at the [edit system accounting] hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
    tacplus {
        server {
            server-address {
                port port-number;
                secret password;
                single-connection;
                timeout seconds;
            }
        }
    }
}
```

This section includes the following topics:



### Specifying Events

To specify the events you want to audit, include the events statement at the [edit system accounting] hierarchy level:

```
[edit system accounting]
events [ events ];
```

*events* is one or more of the following:

- login—Audit logins
- change-log—Audit configuration changes
- interactive-commands—Audit interactive commands (any command-line input)

### Configuring TACACS+ Accounting

To configure TACACS+ server accounting, include the server statement at the [edit system accounting destination tacplus] hierarchy level:

```
[edit system accounting destination tacplus]
server {
    server-address {
        port port-number;
        secret password;
        single-connection;
```

```
        timeout seconds;
    }
}
```

*server-address* specifies the address of the TACACS+ server. To configure multiple TACACS+ servers, include multiple server statements.

**NOTE:** If no TACACS+ servers are configured at the [edit system accounting destination tacplus] statement hierarchy level, the JUNOS software uses the TACACS+ servers configured at the [edit system tacplus-server] hierarchy level.

*port-number* specifies the TACACS+ server port number.

You must specify a secret (password) that the local router passes to the TACACS+ client by including the secret statement. If the password contains spaces, enclose the entire password in quotation marks (" "). The password used by the local router must match that used by the server.

Optionally, you can specify the length of time that the local router waits to receive a response from a TACACS+ server by including the timeout statement. By default, the router waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can maintain one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt, by including the single-connection statement.

To ensure that start and stop requests for accounting of login events are correctly logged in the Accounting file instead of the Administration log file on a TACACS+ server, include either the no-cmd-attribute-value statement or the exclude-cmd-attribute at the [edit system tacplus-options] hierarchy level.

If you use the no-cmd-attribute-value statement, the value of the cmd attribute is set to a null string in the start and stop requests. If you use the exclude-cmd-attribute statement, the cmd attribute is totally excluded from the start and stop requests. Both statements support the correct logging of accounting requests in the Accounting file, instead of the Administration file.

```
[edit system tacplus-options]
(no-cmd-attribute-value | exclude-cmd-attribute);
```

### *Configuring TACACS+ Accounting on a TX Matrix Platform*

On a TX Matrix platform, TACACS+ accounting should be configured only under the groups re0 and re1.

**NOTE:** Accounting should *not* be configured at the [edit system] hierarchy; on a TX Matrix platform, control is done under the switch-card chassis only.

## Enabling the SRC Software

You can enable JUNOS software to work with the Session and Resource Control (SRC) software. The SRC software supports dynamic service activation engine (SAE) functionality on JUNOS routers. To do this, include the following statements at the [edit system services service-deployment] hierarchy level:

```
[edit system services service-deployment]
servers server-address {
    port port-number;
}
source-address source-address;
```

*server-address* is the IPv4 address of the SRC server.

By default, *port-number* is set to 3333 and is a TCP port number.

*source-address* is optional, and is the local IP version 4 (IPv4) address to be used as the source address for traffic to the SRC server.

**NOTE:** By default, when a connection between SRC and a Juniper Networks router is established, the SRC process (sdxd) starts a JUNOScript session as user root. Beginning with JUNOS Release 7.6, you have the option of configuring user sdx with a different classification at the [edit system login] hierarchy level. For more information about configuring user accounts, see "Configuring User Accounts" on page 72.

For more information about SRC software, see the SRC documentation set.

## Configuring the ICMP4 Rate Limit

To limit the rate at which ICMPv4 messages can be generated by the Routing Engine and sent to the Routing Engine, include the icmpv4-rate-limit statement at the [edit system internet-options] hierarchy level:

```
icmpv4-rate-limit {
    bucket-size bucket-size;
    packet-rate packet-rate;
}
```

The bucket size is the the number of seconds in the rate-limiting bucket. The packet rate is the packets earned per second.

## Configuring the ICMPv6 Rate Limit

To limit the rate at which ICMPv6 messages are sent, include the icmpv6-rate-limit statement at the [edit system internet-options] hierarchy level:

```
icmpv6-rate-limit {
    bucket-size bucket-size;
    packet-rate packet-rate;
```

```
}
```

The bucket size is the the number of seconds in the rate-limiting bucket. The packet rate is the packets earned per second.

## Configuring IP-IP Path MTU Discovery

By default, path maximum transmission unit (MTU) discovery on outgoing IP-IP tunnel connections is disabled. To enable IP-IP path MTU discovery, include the ipip-path-mtu-discovery statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
ipip-path-mtu-discovery;
```

To disable IP-IP path MTU discovery, include the no-ipip-path-mtu-discovery statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
no-ipip-path-mtu-discovery;
```

## Configuring TCP MSS for Session Negotiation

During session connection establishment, two peers agree in negotiations to determine the IP segment size of packets that they will exchange during their communication. The TCP MSS (maximum segment size) value in TCP SYN packets specifies the maximum number of bytes that a TCP packet's data field, or segment, can contain. An MSS value that is set too high could result in an IP datagram that is too large to send and that must be fragmented. Fragmentation can incur additional overhead cost and packet loss.

To diminish the likelihood of fragmentation and to protect against packet loss, you can use the tcp-mss statement to specify a lower TCP MSS value. The tcp-mss statement applies to all IPv4 TCP SYN packets traversing all the router's ingress interfaces whose MSS value is higher than the one you specify. You cannot exempt particular ports from its effects.

**NOTE:** The tcp-mss statement is only applicable to J-series Services Routers.

To specify a TCP MSS value to be used, include the following statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
tcp-mss {
   mss-value;
}
```

The value of *mss-value* is a number in the range from 64 through 65535.

To remove the TCP MSS specification from the configuration, use the following command:

```
delete system internet-options tcp-mss
```

For more information about the tcp-mss statement and session negotiation, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

## Configuring IPv6 Path MTU Discovery

By default, Path MTU (PMTU) discovery for IPv6 packets is enabled. To disable IPv6 PMTU discovery, include the no-ipv6-path-mtu-discovery statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
no-ipv6-path-mtu-discovery;
```

To configure IPv6 PMTU discovery timeout in minutes, include the ipv6-path-mtu-discovery-timeout statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
ipv6-path-mtu-discovery-timeout minutes;
```

For details about IPv6 PMTU, see RFC 1981, *Path MTU Discovery for IP version 6*.

## Configuring IPv6 Duplicate Address Detection Transmits

The ipv6-duplicate-addr-detection-transmits statement at the [edit system internet-options] hierarchy level controls the number of attempts for IPv6 duplicate address detection. The default value is 3.

## Configuring Acceptance of IPv6 Packets with Zero Hop-Limit

The ipv6-reject-zero-hop-limit and no-ipv6-reject-zero-hop-limit statements are used to enable and disable rejection of incoming IPv6 packets that have a zero hop-limit value in their header.

By default, such packets are rejected both when they are addressed to the local host and when they are transiting the router. To accept zero hop-limit packets addressed to the local host, include the no-ipv6-reject-zero-hop-limit statement at the [edit system internet-options] hierarchy level. Transit packets are still dropped.

```
{master}[edit]
user@host#
set system internet-options no-ipv6-reject-zero-hop-limit
```

## Configuring GRE Path MTU Discovery

By default, path MTU discovery on outgoing GRE tunnel connections is disabled. To enable GRE path MTU discovery, include the gre-path-mtu-discovery statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
```

```
gre-path-mtu-discovery;
```

To disable GRE path MTU discovery, include the **no-gre-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-gre-path-mtu-discovery;
```

## Configuring Path MTU Discovery

By default, path MTU discovery on outgoing TCP connections is disabled. To enable path MTU discovery, include the **path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
path-mtu-discovery;
```

To disable path MTU discovery on outgoing TCP connections, include the **no-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-path-mtu-discovery;
```

## Configuring Source Quench

By default, Internet Control Message Protocol (ICMP) source quench is disabled. You enable **source quench** when you want the JUNOS software to ignore ICMP source quench messages. To do this, include the **source-quench** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
source-quench;
```

To disable ICMP source quench, include the **no-source-quench** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-source-quench;
```

## Configuring the Router to Drop Packets with the SYN and FIN Bits Set

By default, the router accepts packets that have both the SYN and FIN bits set in the TCP flag. You can configure the router to drop packets with both the SYN and FIN bits set. Accepting packets with the SYN and FIN bits set can result in security vulnerabilities, such as denial-of-service attacks. To configure the router to drop such packets, include the **tcp-drop-synfin-set** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
tcp-drop-synfin-set;
```

## Configuring No TCP RFC 1323 Extensions

To disable RFC 1323 TCP extensions, include the no-tcp-rfc1323 statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
no-tcp-rfc1323;
```

## Configuring No TCP RFC 1323 PAWS Extension

To disable Protection Against Wrapped Sequence (PAWS) number extension (described in RFC 1323, *TCP Extensions for High Performance*), include the no-tcp-rfc1323-paws statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
no-tcp-rfc1323-paws;
```

## Configuring the Range of Port Addresses

By default, the upper range of a port address is 5000. You can increase the range from which the port number can be selected to decrease the probability that someone can determine your port number. To do so, include the source-port statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
source-port upper-limit upper-limit;
```

upper-limit *upper-limit* is the upper limit of a source port address and can be a value from 5000 through 65,355.

## Configuring ARP Learning and Aging

The Address Resolution Protocol (ARP) is a protocol used by IPv4 to map IP network addresses to MAC addresses. This section describes how to set passive ARP learning and ARP aging options for routers. For more information about configuring ATM on Juniper Networks routing platforms, see the *JUNOS Network Interfaces Configuration Guide*.

For more information, see the following sections:

- Configuring Passive ARP Learning for Backup VRRP Routers on page 203
- Adjusting the ARP Aging Timer on page 204

### *Configuring Passive ARP Learning for Backup VRRP Routers*

By default, the backup VRRP router drops ARP requests for the VRRP-IP to VRRP-MAC address translation. The backup router does not learn the ARP (IP-to-MAC address) mappings for the hosts sending the requests. When it detects a failure of the master router and becomes the new master, the backup router must learn all the entries that were present in the ARP cache of the master router. In environments with many directly attached hosts, such as metro Ethernet environments, the number of ARP

entries to learn can be high. This can cause a significant transition delay, during which traffic transmitted to some of the hosts might be dropped.

Passive ARP learning enables the ARP cache in the backup router to hold approximately the same contents as the ARP cache in the master router, thus preventing the problem of learning ARP entries in a burst. To enable passive ARP learning, include the passive-learning statement at the [edit system arp] hierarchy level:

```
[edit system arp]
passive-learning;
```

We recommend setting passive learning on both the backup and master VRRP routers. This prevents the need to intervene manually when the master router becomes the backup router. While a router is operating as the master, the passive learning configuration has no operational impact. The configuration takes effect only when the router is operating as a backup router.

### *Adjusting the ARP Aging Timer*

By default, the ARP aging timer is set at 20 minutes. In environments with many directly attached hosts, such as metro Ethernet environments, increasing the amount of time between ARP updates by configuring the ARP aging timer can improve performance. However, in some scenarios, it might be desirable to lower the ARP aging timer value to prevent the flooding of traffic and improve performance.

In JUNOS Release 9.4 and later, the range of the ARP aging timer is from 1 through 240 minutes.

To configure a system-wide ARP aging timer, include the aging-timer statement at the [edit system arp] hierarchy level:

```
[edit system arp]
aging-timer minutes;
```

You can also configure the ARP aging timer for each logical interface of family type inet. To configure the ARP aging timer at the logical interface level, specify the timer value in minutes at the
[edit system arp aging-timer interface *interface-name*] hierarchy level:

```
[edit system arp aging-timer interface interface-name]
aging-timer-minutes;
```

**NOTE:** If the aging timer value is configured both at the system and the logical interface levels, the value configured at the logical interface level takes precedence for the specific logical interface.

The timer value you configure takes effect as ARP entries expire. Each refreshed ARP entry receives the new timer value. The new timer value does not apply to ARP entries that exist at the time you commit the configuration.

## Configuring System Alarms to Appear Automatically

You can configure J-series Services Routers to execute a show system alarms command whenever a user with the login class admin logs on to the router. To do so, include the login-alarms statement at the [edit system login class admin] hierarchy level:

```
[edit system login class admin]
login-alarms;
```

Table 32 on page 205 describes system alarms that may occur. These alarms are preset and cannot be modified.

**Table 32: System Alarms**

| Alarm Type | Alarm Summary | Remedy |
|---|---|---|
| Configuration | This alarm appears if you have not created a rescue configuration for the router. If you inadvertently commit a configuration that denies management access to the router, you must either connect a console to the router or invoke a rescue configuration. Using a rescue configuration is the recommended method. A rescue configuration is one that you know allows management access to the router. | Create the rescue configuration. For more information, see the *JUNOS CLI User Guide*. |
| License | This alarm appears if you have configured at least one software feature that requires a feature license, but no valid license for the feature is currently installed. | Install a valid license key. |

For more information on system alarms for J-series Services Routers, see the *J-series Services Router Administration Guide*. For more information on the show system alarms command, see the *JUNOS System Basics and Services Command Reference*.

Chapter 11

# Security Configuration Example

This chapter provides an example of a configuration that applies sound security policies so that the router can operate securely. This configuration > is specific to IP version 4 (IPv4).

The final section in this example, "Example: Consolidated Security Configuration" on page 223, shows the complete configuration example.

**NOTE:** For advanced network security, a special version of JUNOS, called JUNOS FIPS is available. For information about how to configure a network of Juniper Networks routers in a FIPS environment, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

The following sections explain how to configure a router securely:



## Configuring System Information

Configure the router name and domain name:

```
[edit]
system {
    host-name Secure-Router;
    domain-name company.com;
    default-address-selection;
}
```

This section includes the following topics:

## *Configuring RADIUS*

The JUNOS software supports two protocols for central authentication of users on multiple routers: Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+). We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and all vendors of these systems support RADIUS.

In the JUNOS model for centralized RADIUS authentication, you create one or more template accounts on the router, and the users' access to the router is configured to use the template account. In this configuration, if the RADIUS server is not reachable, the fallback authentication mechanism is through the local account set up on the router.

```
[edit]
system {
   authentication-order [ radius password ];
   root-authentication {
      encrypted-password "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; # SECRET-DATA
   }
   name-server {
      10.1.1.1;
      10.1.1.2;
   }
}
```

Enable RADIUS authentication and define the shared secret between the client and the server so each know that they are talking to the trusted peer. Define a timeout value for each server so if there is no response within the specified number of seconds, the router can try either the next server or the next authentication mechanism.

```
[edit]
system {
   radius-server {
      10.1.2.1 {
         secret "$9$aH1j8gqQ1sdjerrrhser"; # SECRET-DATA
         timeout 5;
      }
      10.1.2.2 {
         secret "$9$aH1j8gqQ1csdoiuardwefoiud"; # SECRET-DATA
         timeout 5;
      }
   }
}
```

### *Creating Login Classes*

Create several user classes, each with specific privileges. In this example, you configure timeouts to disconnect the class members after a period of inactivity. Users' privilege levels, and therefore the classes of which they are members, should be dependent on their responsibilities within the organization, and the permissions shown here are only examples.

The first class of users (called "observation") can only view statistics and configuration. They are not allowed to modify any configuration. The second class of users (called "operation") can view and modify the configuration. The third class of users (called "engineering") has unlimited access and control.

```
[edit]
system {
   login {
      class observation {
         idle-timeout 5;
         permissions [ view ];
      }
      class operation {
         idle-timeout 5;
         permissions [ admin clear configure interface interface-control network
         reset routing routing-control snmp snmp-control trace-control
         firewall-control rollback ];
      }
      class engineering {
         idle-timeout 5;
         permissions all;
      }
   }
}
```

### *Defining User Login Accounts*

Define the local superuser account. If RADIUS fails or becomes unreachable, revert to the local accounts on the router.

```
[edit]
system {
   login {
      user admin {
         uid 1000;
         class engineering;
         authentication {
            encrypted-password "<PASSWORD>"; # SECRET-DATA
         }
      }
   }
}
```

### *Defining RADIUS Template Accounts*

Define RADIUS template accounts for different users or groups of users:

```
[edit]
system {
   login {
      user observation {
         uid 1001;
         class observation;
      }
      user operation {
         uid 1002;
         class operation;
      }
      user engineering {
         uid 1003;
         class engineering;
      }
   }
}
```

### *Enabling Connection Services*

Enable connection services on the router. SSH provides secure encrypted communications over an insecure network and is therefore useful for inband router management. Like all other types of network-based access, however, SSH access to the router is disabled by default in the JUNOS software. The following configuration enables SSH access and sets optional parameters that can be used to control the number of concurrent SSH sessions and the maximum number of SSH sessions that can be established in one minute. The rate-limit option can be useful in protecting against SYN flood denial-of-service (DoS) attacks on the SSH port.

```
[edit]
system {
   services {
      ssh connection-limit 10 rate-limit 4;
   }
}
```

### *Configuring System Logging*

A file that records when authentication and authorization is granted and rejected, as well as all user commands, provides an excellent way to track all management activity on the router. Checking these files for failed authentication events can help identify attempts to hack into the router. These files can also provide logs of all the command executed on the router and who has performed them. You can review logs of the commands executed on the router and correlate any event in the network with changes made at a particular time. These files are stored locally on the router. Place the firewall logs in a separate system log file.

```
[edit]
system {
   syslog {
      file messages {
         any notice;
         authorization info;
         daemon any;
```

```
        kernel any;
        archive size 10m files 5 no-world-readable;
      }
      file authorization-commands {
        authorization any;
        interactive-commands any;
      }
      file firewall-logs {
        firewall any;
      }
    }
  }
```

### *Configuring the Time Source*

Debugging and troubleshooting are much easier when the timestamps in the log files of all routers are synchronized, because events that span the network can be correlated with synchronous entries in multiple logs. We strongly recommend the using the Network Time Protocol (NTP) to synchronize the system clocks of routers and other network equipment.

By default, NTP operates in an entirely unauthenticated manner. If a malicious attempt to influence the accuracy of a router's clock succeeds, it could have negative effects on system logging, make troubleshooting and intrusion detection more difficult, and impede other management functions.

The following configuration synchronizes all the routes in the network to a single time source. We recommend using authentication to make sure that the NTP peer is trusted. The boot-server statement identifies the server from which the initial time of day and date is obtained when the router boots. The server statement identifies the NTP server used for periodic time synchronization. The authentication-key statement specifies that an HMAC-Message Digest 5 (MD5) scheme is used to hash the key value for authentication, which will prevent the router from synchronizing with a attacker's host posing as the time server.

```
[edit]
system {
  ntp {
    authentication-key 2 type md5 value "$9$aH1j8gqQ1gjyjgjhgjgiiii"; # SECRET-DATA
    boot-server 10.1.4.1;
    server 10.1.4.2;
  }
}
```

## Configuring Interfaces

Configure the interfaces on your router. This example shows configurations for Asynchronous Transfer Mode (ATM), SONET, loopback, and out-of-band management interfaces. For more information about configuring interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

Configure an ATM interface:

```
[edit]
interfaces {
    at-4/0/0 {
        description core-router;
        atm-options {
            vpi 0 maximum-vcs 1024;
            ilmi;
        }
        unit 131 {
            description to-other-core-router;
            encapsulation atm-snap;
            point-to-point;
            vci 0.131;
            family inet {
                address 12.1.1.1/30;
            }
            family iso;
        }
    }
}
```

The fxp0 interface can be used for out-of-band management. However, because most service providers use inband communication for management (because of lower operating costs), you can disable this interface to make the router more secure.

```
[edit]
interfaces {
    fxp0 {
        disable;
    }
}
```

Configure the loopback interface. To protect the Routing Engine, apply a firewall filter to the router's loopback interface. This filter, which you define at the [edit firewall] hierarchy level, checks all traffic destined for the Routing Engine that enters the router from the customer interfaces. Adding or modifying filters for every interface on the router is not necessary.

```
[edit]
interfaces {
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input protect-routing-engine;
                }
                address 10.10.5.1/32;
            }
            family iso {
                address 48.0005.80dd.f900.0000.0001.0001.0000.0000.011.00;
            }
        }
    }
}
```

Configure a SONET interface:

```
[edit]
interfaces {
    so-2/0/0 {
        description To-other-router;
        clocking external;
        sonet-options {
            fcs 32;
            payload-scrambler;
        }
        unit 0 {
            family inet {
                address 10.1.5.1/30;
            }
            family iso;
        }
    }
}
```

## Configuring SNMP

Configure Simple Network Management Protocol version 3 (SNMPv3):

```
[edit snmp]
engine-id {
    use-fxp0-mac-address;
}
view jnxAlarms {
    oid 1.3.6.1.4.1.2636.3.4 include;
}
view interfaces {
    oid 1.3.6.1.2.1.2 include;
}
view ping-mib {
    oid 1.3.6.1.2.1.80 include;
}
[edit snmp v3]
notify n1 {
    tag router1; # Identifies a set of target addresses
    type trap;# Defines type of notification
}
notify n2 {
    tag host1;
    type trap;
}
notify-filter nf1 {
    oid .1 include; # Defines which traps (or which objects for which traps) are sent. In
        this case, includes all traps
}
notify-filter nf2 {
    oid 1.3.6.1.4.1 include; # Sends enterprise-specific traps only
}
notify-filter nf3 {
    oid 1.3.6.1.2.1.1.5 include; # Sends BGP traps only
```

```
}
snmp-community index1 {
   community-name "$9$JOZi.QF/AtOz3"; # SECRET-DATA
   security-name john; # Matches the security name at the target-parameters
   tag host1; # Finds the addresses that can be used with this community string
}
target-address ta1 { # Associates the target address with the group san-francisco
address 10.1.1.1;
address-mask 255.255.255.0; # Defines the range of addresses
port 162;
tag-list router1;
target-parameters tp1;# Applies configured target parameters
target-address ta2 {
   address 10.1.1.2;
   address-mask 255.255.255.0;
   port 162;
   tag-list host1;
   target-parameters tp2;
}
target-address ta3 {
   address 10.1.1.3;
   address-mask 255.255.255.0;
   port 162;
   tag-list [router1 host1];
   target-parameters tp3;
}
target-parameters tp1 {# Defines the target parameters
notify-filter nf1; # Specifies which notify filter to apply
parameters {
   message-processing-model v1;
   security-model v1‘;
   security-level none;
   security-name john; # Matches the security name configured at the [edit snmp v3
      snmp-community community-index] hierarchy level
}
}# level
target-parameters tp2 {
   notify-filter nf2;
   parameters {
      message-processing-model v1;
      security-model v1;
      security-level none;
      security-name john;
   }
}
target-parameters tp3 {
   notify-filter nf3;
   parameters {
      message-processing-model v1;
      security-model v1;
      security-level none;
      security-name john;
   }
}
usm {
   local-engine { # Defines authentication and encryption for
```

```
    user user1 { # SNMPv3 users
    authentication-md5 {
        authentication-password authentication-password;
    }
    privacy-des {
        privacy-password password;
    }
}
user user2 {
    authentication-sha {
        authentication-password authentication-password;
    }
    privacy-none;
}
user user3 {
    authentication-none;
    privacy-none;
}
user user4 {
    authentication-md5 {
        authentication-password authentication-password;
    }
    privacy-3des {
        privacy-password password;
    }
}
user user5 {
    authentication-sha {
        authentication-password authentication-password;
    }
    privacy-aes128 {
        privacy-password password;
    }
}
vacm {
    access {
        group san-francisco {# Defines the access privileges for the group
        default-context-prefix { # san-francisco
        security-model v1 {
            security-level none {
                notify-view ping-mib;
                read-view interfaces;
                write-view jnxAlarms;
            }
        }
    }
}
security-to-group {
    security-model v1 {
        security-name john {# Assigns john to the security group san-francisco
        group san-francisco;
    }
    security-name bob {
        group new-york;
    }
    security-name elizabeth {
```

```
        group chicago;
    }
}
```

For more information about configuring SNMP, see the *JUNOS Network Management Configuration Guide*.

## Configuring Protocol-Independent Routing Properties

Configure a router ID and autonomous system (AS) number for Border Gateway Protocol (BGP):

```
[edit]
routing-options {
    router-id 10.1.7.1;
    autonomous-system 222;
}
```

Configure martian addresses, which are reserved host or network addresses about which all routing information should be ignored. By default, the JUNOS software blocks the following martian addresses: 0.0.0.0/8, 127.0.0.0/8, 128.0.0.0/16, 191.255.0.0/16, 192.0.0.0/24, 223.255.55.0/24, and 240.0.0.0/4. It is also a good idea to block private address space (addresses defined in RFC 1918). You can add these addresses and other martian addresses to the default martian addresses.

```
[edit]
routing-options {
    martians {
        1.0.0.0/8 exact;
        10.0.0.0/8 exact;
        19.255.0.0/16 exact;
        59.0.0.0/8 exact;
        129.156.0.0/16 exact;
        172.16.0.0/12 exact;
        192.0.2.0/24 exact;
        192.5.0.0/24 exact;
        192.9.200.0/24 exact;
        192.9.99.0/24 exact;
        192.168.0.0/16 exact;
        224.0.0.0/3 exact;
    }
}
```

For more information about configuring protocol-independent routing properties, see the *JUNOS Routing Protocols Configuration Guide*.

### *Reserved IRI IP Addresses*

A number of interception related information (IRI) IP addresses, such as 128.0.0.1, are reserved for internal communication. 128.0.0.1 is the base of the IRI IP address. The upper limit of this range depends on the chassis configuration of the router and may use 129.x.x.x, 130.x.x.x, and so on. Use the CLI command show route table

__juniper_private1__ to show the router's configured IP addresses, including the reserved IRI IP addresses.

### Sample Output

```
user@host> show route table __juniper_private1__
__juniper_private1__.inet.0: 8 destinations, 8 routes (5 active, 0 holddown, 3
hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/8          *[Direct/0] 7w1d 03:24:45
                     > via fxp1.0
10.0.0.1/32         *[Local/0] 7w1d 03:22:48
                       Local via sp-1/2/0.16383
10.0.0.4/32         *[Local/0] 7w1d 03:24:45
                       Local via fxp1.0
10.0.0.34/32        *[Direct/0] 7w1d 03:22:32
                     > via sp-1/2/0.16383
128.0.0.0/2         *[Direct/0] 7w1d 03:24:45
                     > via fxp1.0

__juniper_private1__.inet6.0: 4 destinations, 4 routes (4 active, 0 holddown, 0
hidden)
+ = Active Route, - = Last Active, * = Both

fe80::/64           *[Direct/0] 7w1d 03:24:45
                     > via fxp1.0
fe80::200:ff:fe00:4/128
                    *[Local/0] 7w1d 03:24:45
                       Local via fxp1.0
fec0::/64           *[Direct/0] 7w1d 03:24:45
                     > via fxp1.0
fec0::a:0:0:4/128   *[Local/0] 7w1d 03:24:45
                       Local via fxp1.0
```

## Configuring Routing Protocols

The main task of a router is to use its routing and forwarding tables to forward user traffic to its intended destination. Attackers can send forged routing protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn can degrade the functionality of the router and the network. To prevent such attacks, routers must ensure that they form routing protocol relationships (peering or neighboring relationships) to trusted peers. One way of doing this is by authenticating routing protocol messages. We strongly recommend using authentication when configuring routing protocols. The JUNOS software supports HMAC-MD5 authentication for BGP, Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and Resource Reservation Protocol (RSVP). HMAC-MD5 uses a secret key that is combined with the data being transmitted to compute a hash. The computed hash is transmitted along with the data. The receiver uses the matching key to recompute and validate the message hash. If an attacker has forged or modified the message, the hash will not match and the data will be discarded.

In this example, we configure BGP and, as the interior gateway protocol (IGP), IS-IS. If you use OSPF, configure it similarly to the IS-IS configuration shown.

This section includes the following topics:



For more information about configuring BGP and IS-IS, see the *JUNOS Routing Protocols Configuration Guide*.

## Configuring BGP

The following example shows the configuration of a single authentication key for the BGP peer group internal peers. You can also configure BGP authentication at the neighbor or routing instance levels, or for all BGP sessions. As with any security configuration, there is a tradeoff between the degree of granularity (and to some extent the degree of security) and the amount of management necessary to maintain the system. This example also configures a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
    bgp {
        group ibgp {
            type internal;
            traceoptions {
                file bgp-trace size 1m files 10;
                flag state;
                flag general;
            }
            local-address 10.10.5.1;
            log-updown;
            neighbor 10.2.1.1;
            authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiii";
        }
        group ebgp {
            type external;
            traceoptions {
                file ebgp-trace size 10m files 10;
                flag state;
                flag general;
            }
            local-address 10.10.5.1;
            log-updown;
            peer-as 2;
            neighbor 10.2.1.2;
            authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiii";
        }
    }
}
```

### *Configuring IS-IS*

Although all JUNOS IGPs support authentication, some are inherently more secure than others. Most service providers use OSPF or IS-IS to allow fast internal convergence and scalability and to use traffic engineering capabilities with Multiprotocol Label Switching (MPLS). Because IS-IS does not operate at the network layer, it is more difficult to spoof than OSPF, which is encapsulated in IP and is therefore subject to remote spoofing and DoS attacks. This example also configures a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
    isis {
        authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiii"; # SECRET-DATA
        authentication-type md5;
        traceoptions {
            file isis-trace size 10m files 10;
            flag normal;
            flag error;
        }
        interface at-0/0/0.131 {
            lsp-interval 50;
            level 2 disable;
            level 1 {
                metric 3;
                hello-interval 5;
                hold-time 60;
            }
        }
        interface lo0.0 {
            passive;
        }
    }
}
```

## Configuring Firewalls

To configure firewall policies, configure the trusted source addresses with which each protocol or service wants to communicate. Once you define the prefix list, you apply it in the filter definition at the [edit firewall] hierarchy level.

For more information about configuring firewalls, see the *JUNOS Policy Framework Configuration Guide*.

```
[edit]
policy-options {
    prefix-list ssh-addresses {
        1.1.9.0/24;
    }
    prefix-list bgp-addresses {
```

```
        10.2.1.0/24;
    }
    prefix-list ntp-addresses {
        10.1.4.0/24;
    }
    prefix-list snmp-addresses {
        10.1.6.0/24;
    }
    prefix-list dns-address {
        10.1.1.0/24;
    }
    prefix-list radius-address {
        10.1.2.0/24;
    }
}
```

The following firewall filter protects the Routing Engine. To protect the Routing Engine, it is important to constrain the traffic load from each of the allowed services. Rate-limiting control traffic helps protect the Routing Engine from attack packets that are forged such that they appear to be legitimate traffic and are then sent at such a high rate as to cause a DoS attack.

Routing and control traffic are essential to proper functioning of the router, and rapid convergence of routing protocols is crucial for stabilizing the network during times of network instability. While it might seem desirable to limit the amount of routing protocol traffic to protect against various types of attacks, it is very difficult to determine a fixed maximum rate for protocol traffic, because it depends upon the number of peers and adjacencies, which varies over time. Therefore, it is best not to rate-limit routing protocol traffic.

By contrast, because management traffic is less essential and more deterministic than routing protocol traffic, it can be policed to a fixed rate, to prevent it from consuming resources necessary for less flexible traffic. We recommend allocating a fixed amount of bandwidth to each type of management traffic so that an attacker cannot consume all the router's CPU if an attack is launched using any single service.

```
[edit]
firewall {
    filter protect-routing-engine {
        policer ssh-policer {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 15k;
            }
            then discard;
        }
        policer small-bandwidth-policer {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 15k;
            }
            then discard;
        }
        policer snmp-policer {
```

```
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
policer ntp-policer {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
policer dns-policer {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
policer radius-policer {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
policer tcp-policer {
    if-exceeding {
        bandwidth-limit 500k;
        burst-size-limit 15k;
    }
    then discard;
}
/* The following terms accept traffic only from the trusted sources. The trusted
    traffic is rate-limited with the exception of the routing protocols. */
/* The following term protects against ICMP flooding attacks against the Routing
    Engine. */
term icmp {
    from {
        protocol icmp;
        icmp-type [ echo-request echo-reply unreachable time-exceeded ];
    }
    then {
        policer small-bandwidth-policer;
        accept;
    }
}
term tcp-connection {
    from {
        source-prefix-list {
            ssh-addresses;
            bgp-addresses;
        }
        protocol tcp;
        tcp-flags "(syn & !ack) | fin | rst";
```

```
    }
    then {
        policer tcp-policer;
        accept;
    }
}
/* The following term protects SSH traffic destined for the Routing Engine. */
term ssh {
    from {
        source-prefix-list {
            ssh-addresses;
        }
        protocol tcp;
        port [ ssh telnet ];
    }
    policer ssh-policer;
    then accept;
}
/* The following term protects BGP traffic destined for the Routing Engine. */
term bgp {
    from {
        source-prefix-list {
            bgp-addresses;
        }
        protocol tcp;
        port bgp;
    }
    then accept;
}
term snmp {
    from {
        source-prefix-list {
            snmp-addresses;
        }
        protocol udp;
        port snmp;
    }
    then {
        policer snmp-policer;
        accept;
    }
}
term ntp {
    from {
        source-prefix-list {
            ntp-addresses;
        }
        protocol udp;
        port ntp;
    }
    then {
        policer ntp-policer;
        accept;
    }
}
term dns {
```

```
            from {
                source-address {
                    dns-addresses;
                }
                protocol udp;
                port domain;
            }
            then {
                policer dns-policer;
                accept;
            }
        }
        term radius {
            from {
                source-address {
                    radius-addresses;
                }
                protocol udp;
                port radius;
            }
            then {
                policer radius-policer;
                accept;
            }
        }
        term trace-route {
            from {
                protocol udp;
                destination-port 33434-33523;
            }
            then {
                policer small-bandwidth-policer;
                accept;
            }
            /* All other traffic that is not trusted is silently dropped. We recommend logging
               the denied traffic for analysis purposes. */
            term everything-else {
                then {
                    syslog;
                    log;
                    discard;
                }
            }
        }
    }
}
```

## Example: Consolidated Security Configuration

**Basic System Information**

```
system {
    host-name Secure-Router;
    domain-name company.com;
    default-address-selection;
}
```

**RADIUS**

```
authentication-order [ radius password ];
root-authentication {
    encrypted-password "$9$aH1j8gqQ1gjyjgjhgjgiiii"; # SECRET-DATA
}
name-server {
    10.1.1.1;
    10.1.1.2;
}
radius-server {
    10.1.2.1 {
        secret "$9$aH1j8gqQ1sdjerrrhser"; # SECRET-DATA
        timeout 5;
    }
    10.1.2.2 {
        secret "$9$aH1j8gqQ1csdoiuardwefoiud"; # SECRET-DATA
        timeout 5;
    }
}
```

**Login Classes**

```
login {
    class observation {
        idle-timeout 5;
        permissions [ view ];
    }
    class operation {
        idle-timeout 5;
        permissions [ admin clear configure interface interface-control network
        reset routing routing-control snmp snmp-control trace-control
        firewall-control rollback ];
    }
    class engineering {
        idle-timeout 5;
        permissions all;
    }
}
```

**User Login Accounts**

```
user admin {
    uid 1000;
    class engineering;
    authentication {
        encrypted-password "<PASSWORD>"; # SECRET-DATA
    }
}
```

**RADIUS Template Accounts**

```
user observation {
    uid 1001;
    class observation;
}
user operation {
    uid 1002;
    class operation;
}
user engineering {
    uid 1003;
    class engineering;
```

```
}
```

**Connection Services**

```
services {
    ssh connection-limit 10 rate-limit 4;
}
```

**System Logging**

```
syslog {
    file messages {
        any notice;
        authorization info;
        daemon any;
        kernel any;
        archive size 10m files 5 no-world-readable;
    }
    file authorization-commands {
        authorization any;
        interactive-commands any;
    }
    file firewall-logs {
        firewall any;
    }
}
```

**Time Source**

```
ntp {
    authentication-key 2 type md5 value "$9$aH1j8gqQ1gjyjgjhgjgiiii"; \
    #  SECRET-DATA
    boot-server 10.1.4.1;
    server 10.1.4.2;
}
```

**Interfaces**

```
interfaces {
    at-4/0/0 {
        description core router;
        atm-options {
            vpi 0 maximum-vcs 1024;
            ilmi;
        }
        unit 131 {
            description to-other-core-router;
            encapsulation atm-snap;
            point-to-point;
            vci 0.131;
            family inet {
                address 12.1.1.1/30;
            }
            family iso;
        }
    }
    fxp0 {
        disable;
    }
    lo0 {
        unit 0 {
            family inet {
```

```
            filter {
               input protect-routing-engine;
            }
            address 10.10.5.1/32;
         }
         family iso {
            address 48.0005.80dd.f900.0000.0001.0001.0000.0000.011.00;
         }
      }
   }
   so-2/0/0 {
      description To-other-router;
      clocking external;
      sonet-options {
         fcs 32;
         payload-scrambler;
      }
      unit 0 {
         family inet {
            address 10.1.5.1/30;
         }
         family iso;
      }
   }
}
```

**SNMP**

```
[edit snmp]
engine-id {
   use-fxp0-mac-address;
}
view jnxAlarms {
   oid .1.3.6.1.4.1.2636.3.4 include;
}
view interfaces {
   oid .1.3.6.1.2.1.2 include;
}
view ping-mib {
   oid .1.3.6.1.2.1.80 include;
}
[edit snmp v3]
notify n1 {
   tag router1;              # Identifies a set of target addresses
   type trap;                # Defines type of notification
}
notify n2 {
   tag host1;
   type trap;
}
notify-filter nf1 {
   oid 1 include;
      # Defines which (or the objects for which) traps are sent.
      #In this case, includes all traps
}
notify-filter nf2 {
   oid 1.3.6.1.4.1 include;      # Sends enterprise-specific traps only
```

```
}
notify-filter nf3 {
   oid 1.3.6.1.2.1.1.5 include;   # Sends BGP traps only
}
snmp-community index1 {
   community-name "$9$JOZi.QF/AtOz3";     # SECRET-DATA
   security-name john;       # Matches the security name at the target parameters
   tag host1; # Finds the addresses that can be used with
      # this community string
}
target-address ta1 { # Associates the target address with the group san-francisco
address 10.1.1.1;
address-mask 255.255.255.0; # Defines the range of addresses
port 162;
tag-list router1;
target-parameters tp1; # Applies configured target parameters
target-address ta2 {
   address 10.1.1.2;
   address-mask 255.255.255.0;
   port 162;
   tag-list host1;
   target-parameters tp2;
}
target-address ta3 {
   address 10.1.1.3;
   address-mask 255.255.255.0;
   port 162;
   tag-list [router1 host1];
   target-parameters tp3;
}
target-parameters tp1 {          # Defines the target parameters
notify-filter nf1;              # Specifies which notify filter to apply
parameters {
   message-processing-model v1;
   security-model v1;
   security-level none;
   security-name john;      # Matches the security name configured at the
      # [edit snmp v3 snmp-community community-index]
      # hierarchy level
}
} # hierarchy level
target-parameters tp2 {
   notify-filter nf2;
   parameters {
      message-processing-model v1;
      security-model v1;
      security-level none;
      security-name john;
   }
}
target-parameters tp3 {
   notify-filter nf3;
   parameters {
      message-processing-model v1;
      security-model v1;
      security-level none;
```

```
        security-name john;
    }
}
usm {
    local-engine {          #Defines authentication and encryption for SNMP3 users.
    user user1 {
        authentication-md5 {
            authentication-password authentication-password;
        }
        privacy-des {
            privacy-password privacy-password;
        }
    }
    user user2 {
        authentication-sha {
            authentication-password authentication-password;
        }
        privacy-none;
    }
    user user3 {
        authentication-none;
        privacy-none;
    }
    user user4 {
        authentication-md5 {
            authentication-password authentication-password;
        }
        privacy-3des {
            privacy-password password;
        }
    }
    user user5 {
        authentication-sha {
            authentication-password authentication-password;
        }
        privacy-aes128 {
            privacy-password password;
        }
    }
}
vacm {
    access {
        group san-francisco {           # Defines the access privileges for the group
        default-context-prefix {        # san-francisco
        security-model v1 {
            security-level none {
                notify-view ping-mib;
                read-view interfaces;
                write-view jnxAlarms;
            }
        }
    }
}
security-to-group {
    security-model v1 {
        security-name john {            # Assigns john to the security group
```

```
        group san-francisco;        # san-francisco
        security-name bob {
            group new-york;
        }
        security-name elizabeth {
            group chicago;
        }
    }
}
```

**Protocol-Independent Routing Properties**

```
routing-options {
    router-id 10.1.7.1;
    autonomous-system 222;
    martians {
        1.0.0.0/8 exact;
        10.0.0.0/8 exact;
        19.255.0.0/16 exact;
        59.0.0.0/8 exact;
        129.156.0.0/16 exact;
        172.16.0.0/12 exact;
        192.0.2.0/24 exact;
        192.5.0.0/24 exact;
        192.9.200.0/24 exact;
        192.9.99.0/24 exact;
        192.168.0.0/16 exact;
        224.0.0.0/3 exact;
    }
}
```

**Routing Protocols**

```
protocols {
}
```

**BGP**

```
bgp {
    group ibgp {
        type internal;
        traceoptions {
            file bgp-trace size 1m files 10;
            flag state;
            flag general;
        }
        local-address 10.10.5.1;
        log-updown;
        neighbor 10.2.1.1;
        authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiii";
    }
    group ebgp {
        type external;
        traceoptions {
            file ebgp-trace size 10m files 10;
            flag state;
            flag general;
        }
        local-address 10.10.5.1;
        log-updown;
        peer-as 2;
```

```
        neighbor 10.2.1.2;
        authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiii";
    }
}
```

**IS-IS**

```
isis {
    authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiii"; # SECRET-DATA
    authentication-type md5;
    traceoptions {
        file isis-trace size 10m files 10;
        flag normal;
        flag error;
    }
    interface at-0/0/0.131 {
        lsp-interval 50;
        level 2 disable;
        level 1 {
            metric 3;
            hello-interval 5;
            hold-time 60;
        }
    }
    interface lo0.0 {
        passive;
    }
}
```

**Firewall Policies**

```
policy-options {
    prefix-list ssh-addresses {
        1.1.9.0/24
    }
    prefix-list bgp-addresses {
        10.2.1.0/24;
    }
    prefix-list ntp-addresses {
        10.1.4.0/24
    }
    prefix-list snmp-addresses {
        10.1.6.0/24;
    }
    prefix-list dns-addresses {
        10.1.1.0/24;
    }
    prefix-list radius-addresses {
        10.1.2.0/24;
    }
}
```

**Firewall Filters**

```
firewall {
    filter protect-routing-engine {
        term icmp {
            from {
                protocol icmp;
                icmp-type [ echo-request echo-reply unreachable time-exceeded ];
            }
```

```
    then {
        policer small-bandwidth-policer;
        accept;
    }
}
term tcp-connection {
    from {
        source-prefix-list {
            ssh-addresses;
            bgp-addresses;
        }
        protocol tcp;
        tcp-flags "(syn & !ack) | fin | rst";
    }
    then {
        policer tcp-policer;
        accept;
    }
}
term ssh {
    from {
        source-prefix-list {
            ssh-addresses;
        }
        protocol tcp;
        port [ ssh telnet ];
    }
    policer ssh-policer;
    then accept;
}
term bgp {
    from {
        source-prefix-list {
            bgp-addresses;
        }
        protocol tcp;
        port bgp;
        }
        then accept;
        }
    }
term snmp {
    from {
        source-prefix-list {
            snmp-addresses;
        }
        protocol udp;
        port snmp;
    }
    then {
        policer snmp-policer;
        accept;
    }
}
term ntp {
    from {
```

```
            source-prefix-list {
                ntp-addresses;
            }
            protocol udp;
            port ntp;
        }
        then {
            policer ntp-policer;
            accept;
        }
    }
    term dns {
        from {
            source-address {
                dns-addresses;
            }
            protocol udp;
            port domain;
        }
        then {
            policer dns-policer;
            accept;
        }
    }
    term radius {
        from {
            source-prefix-list {
                radius-addresses;
            }
            protocol udp;
            port radius;
        }
        then {
            policer radius-policer;
            accept;
        }
    }
    term trace-route {
        from {
            protocol udp;
            destination-port 33434-33523;
        }
        then {
            policer small-bandwidth-policer;
            accept;
        }
    }
    term everything-else {
        then {
            syslog;
            log;
            discard;
        }
    }
}
    policer ssh-policer {
```

```
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 15k;
            }
            then discard;
        }
        policer small-bandwidth-policer {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 15k;
            }
            then discard;
        }
        policer snmp-policer {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 15k;
            }
            then discard;
        }
        policer ntp-policer {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 15k;
            }
            then discard;
        }
        policer dns-policer {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 15k;
            }
            then discard;
        }
        policer radius-policer {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 15k;
            }
            then discard;
        }
        policer tcp-policer {
            if-exceeding {
                bandwidth-limit 500k;
                burst-size-limit 15k;
            }
            then discard;
        }
    }
```

Chapter 12

# Summary of System Management Configuration Statements

The following sections explain each of the system management configuration statements. The statements are organized alphabetically.

## accounting

**Syntax**

```
accounting {
    events [ login change-log interactive-commands ];
    destination {
        radius {
            server {
                server-address {
                    accounting-port port-number;
                    secret password;
                    source-address address;
                    retry number;
                    timeout seconds;
                }
            }
        }
        tacplus {
            server {
                server-address {
                    port port-number;
                    secret password;
                    single-connection;
                    timeout seconds;
                }
            }
        }
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure audit of TACACS+ or RADIUS authentication events, configuration changes, and interactive commands.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring RADIUS System Accounting” on page 194 and “Configuring TACACS+ System Accounting” on page 197.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## accounting-port

**Syntax** accounting-port *port-number*;

**Hierarchy Level** [edit system accounting destination radius server *server-address*],
[edit system radius-server *server-address*]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure the accounting port number on which to contact the RADIUS server.

**Options** *number*—Port number on which to contact the RADIUS server.
**Default:** 1813

**Usage Guidelines** See and "Configuring RADIUS Authentication" on page 77 and "Configuring RADIUS System Accounting" on page 194.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## allow-commands

**Syntax** allow-commands "*regular-expression*";

**Hierarchy Level** [edit system login class *class-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify the operational mode commands that members of a login class can use.

**Default** If you omit this statement and the deny-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.

**Options** *regular-expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

**Usage Guidelines** See "Specifying Operational Mode Commands" on page 65.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** deny-commands, user

## allow-configuration

**Syntax** allow-configuration "*regular-expression*";

**Hierarchy Level** [edit system login class *class-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify the configuration mode commands that members of a login class can use.

**Default** If you omit this statement and the deny-configuration statement, users can issue only those commands for which they have access privileges through the permissions statement.

**Options** *regular-expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

**Usage Guidelines** See "Specifying Operational Mode Commands" on page 65.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** deny-commands, user

## allow-transients

**Syntax** allow-transients;

**Hierarchy Level** [edit system scripts commit]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For JUNOS commit scripts, enable transient configuration changes to be committed.

**Default** Transient changes are disabled by default. If you do not include the allow-transients statement, and an enabled script generates transient changes, the CLI generates an error message and the commit operation does not succeed.

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

## announcement

**Syntax** announcement *text*;

**Hierarchy Level** [edit system login]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a system login announcement. This announcement appears after a user logs in.

**Options** *text*—Text of the announcement. If the text contains any spaces, enclose it in quotation marks.

**Usage Guidelines** See "Configuring a System Login Announcement" on page 188.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration

**Related Topics** message

## archival

**Syntax**
```
archival {
   configuration {
      transfer-interval interval;
      transfer-on-commit;
      archive-sites {
         ftp://username:<password>@<host>:<port>/<url-path>;
         scp://<username>:<password>@<host>:<port>/<url-path>;
      }
   }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4

**Description** Configure copying of the currently active configuration to an archive site. The remaining statements are described separately.

**Usage Guidelines** See "Configuring a Router to Transfer Its Configuration to an Archive Site" on page 192.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## archive

See the following sections:

- archive (All System Log Files) on page 240
- archive (Individual System Log File) on page 240

### *archive (All System Log Files)*

**Syntax**

```
archive {
    files number;
    size size;
    (world-readable | no-world-readable);
}
```

**Hierarchy Level** [edit system syslog],

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure archiving of all system log files. The remaining statements are described separately.

**Usage Guidelines** See "Specifying Log File Size, Number, and Archiving Properties" on page 123.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

### *archive (Individual System Log File)*

**Syntax**

```
archive {
    archive-sites {
        site-name;
    }
    files number;
    size size;
    start-time date.time;
    transfer-interval interval;
    (world-readable | no-world-readable);
}
```

**Hierarchy Level** [edit system syslog file *filename*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure archiving of specific system log files. The remaining statements are described separately.

**Usage Guidelines** See "Specifying Log File Size, Number, and Archiving Properties" on page 123.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## archive-sites

See the following sections:

- archive-sites (Configuration) on page 241
- archive-sites (System Log) on page 242

### *archive-sites (Configuration)*

**Syntax**

```
archive-sites {
    ftp://username@host:<port>url-path password password;
    http://username@host:<port>url-path password password;
    scp://username@host:<port>url-path password password;
    file://<path>/<filename>;
}
```

**Hierarchy Level** [edit system archival configuration]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify where to transfer the current configuration files. When specifying a URL in a JUNOS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example, "scp://*username*<:*password*>@[*ipv6-host-address*]<:*port*>/*url-path*"

If you specify more than one archive site, the router attempts to transfer the configuration files to the first archive site in the list, moving to the next only if the transfer fails. The format for the destination filename is *router-name*_juniper.conf[.gz]_*YYYYMMDD_HHMMSS*.

**NOTE:** The time included in the destination filename is always in Coordinated Universal Time (UTC) regardless of whether the time on the router is configured as UTC or the local time zone. The default time zone on the router is UTC.

**Usage Guidelines** See "Configuring Archive Sites for Configuration Files" on page 193.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** transfer-on-commit, transfer-on-commit, and configuration

## *archive-sites (System Log)*

**Syntax**
```
archive-sites {
    site-name;
}
```

**Hierarchy Level** [edit system file *filename* archive]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** Configure an archive site. If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the filename specified at the [edit system syslog] hierarchy level.

**Options** *site-name*—Any valid FTP URL to a destination. For information about how to specify valid FTP URLs, see "Specifying Filenames and URLs" on page 36.

**Usage Guidelines** See "Configuring Archive Sites for Configuration Files" on page 193.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## arp

**Syntax**

```
arp {
    passive-learning;
    aging-timer minutes;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4

**Description** Specify ARP options. You can enable backup VRRP routers to learn ARP requests for VRRP-IP to VRRP-MAC address translation. You can also set the time interval between ARP updates.

**Options**

passive-learning—Configures backup VRRP routers to learn the ARP mappings (IP-to-MAC address) for hosts sending the requests. By default, the backup VRRP router drops these requests; therefore, if the master router fails, the backup router must learn all entries present in the ARP cache of the master router. Configuring passive learning reduces transition delay when the backup router is activated.

aging-timer—Time interval in minutes between ARP updates. In environments where the number of ARP entries to update is high (for example, metro Ethernet environments), increasing the time between updates can improve system performance.
**Default:** 20 minutes
**Range:** 1 to 240 minutes

**Usage Guidelines** See *JUNOS Network Interfaces Configuration Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** Configuring ARP Learning and Aging on page 203.

## authentication

See the following sections:

- authentication (Login) on page 244
- authentication (Subscriber Access Management) on page 245

### *authentication (Login)*

**Syntax**

```
authentication {
   (encrypted-password "password" | plain-text-password);
   ssh-dsa "public-key";
   ssh-rsa "public-key";
}
```

**Hierarchy Level** [edit system login user *username*]

**Release Information** Statement introduced before JUNOS Release 7.4

**Description** Authentication methods that a user can use to log in to the router. You can assign multiple authentication methods to a single user.

**Options**

encrypted-password "*password*"—Use Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

plain-text-password—Use a plain-text password. The command-line interface (CLI) prompts you for the password and then encrypts it.

ssh-dsa "*public-key*"—SSH version 2 authentication. Specify the SSH public key. You can specify one or more public keys for each user.

ssh-rsa "*public-key*"—SSH version 1 and SSH version 2 authentication. Specify the SSH public key. You can specify one or more public keys for each user.

**Usage Guidelines** See “Configuring User Accounts” on page 72.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** root-authentication

## *authentication (Subscriber Access Management)*

**Syntax**

```
authentication {
    password password-string;
    username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
        user-prefix user-prefix-string;
    }
}
```

**Hierarchy Level**

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
[edit logical-systems *logical-system-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server group *group-name*]

**Release Information**

Statement introduced in JUNOS Release 9.1.

**Description**

Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.

The statements are explained separately.

**Usage Guidelines**

See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level**

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## authentication-key

**Syntax** authentication-key *key-number* type *type* value *password*;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure Network Time Protocol (NTP) authentication keys so that the router can send authenticated packets. If you configure the router to operate in authenticated mode, you must configure a key.

Both the keys and the authentication scheme (MD5) must be identical between a set of peers sharing the same key number.

**Options** *key-number*—Positive integer that identifies the key.

type *type*—Authentication type. It can only be md5.

value *password*—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.

**Usage Guidelines** See "Configuring NTP Authentication Keys" on page 105.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** broadcast, peer, server, trusted-key

## authentication-order

**Syntax** authentication-order [ *authentication-methods* ];

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.

**Default** If you do not include the authentication-order statement, users are verified based on their configured passwords.

**Options** *authentication-methods*—One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following:

- password—Verify the user using the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.
- radius—Verify the user using RADIUS authentication services.
- tacplus—Verify the user using TACACS+ authentication services.

**Usage Guidelines** See "Configuring the Authentication Order" on page 89.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## autoinstallation

**Syntax**

```
autoinstallation {
    interfaces {
        interface-name {
            bootp;
            rarp;
            slarp;
        }
    }
    configuration-servers {
        url;
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Download a configuration file automatically from an FTP, Hypertext Transfer Protocol (HTTP), or Trivial FTP (TFTP) server. When you power on a J-series Services Router configured for autoinstallation, it requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server. Once the router has an address, it sends a request to a configuration server and downloads and installs a configuration.

The remaining statements are explained separately.

**Usage Guidelines** See the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** configuration-servers, idle-timeout

## auxiliary

**Syntax**
```
auxiliary {
    type terminal-type;
}
```

**Hierarchy Level** [edit system ports]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the characteristics of the auxiliary port, which is on the router's craft interface.

**Default** The auxiliary port is disabled.

**Options** type *terminal-type*—Type of terminal that is connected to the port.
**Range:** ansi, vt100, small-xterm, xterm
**Default:** The terminal type is unknown, and the user is prompted for the terminal type.

**Usage Guidelines** See "Configuring Console and Auxiliary Port Properties" on page 142.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## backup-router

**Syntax** backup-router *address* <destination *destination-address*>;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Set a default router (running IP version 4 [IPv4]) to use while the local router (running IPv4) is booting and if the routing protocol processes fail to start. The JUNOS software removes the route to this router as soon as the software starts.

**Options** *address*—Address of the default router.

destination *destination-address*—(Optional) Destination address that is reachable through the backup router. Include this option to achieve network reachability while loading, configuring, and recovering the router, but without the risk of installing a default route in the forwarding table.
**Default:** All hosts (default route) are reachable through the backup router.

**Usage Guidelines** See "Configuring a Backup Router" on page 50.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## boot-file

**Syntax** boot-file *filename*;

**Hierarchy Level** [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup.

**Options** *filename*—The location of the boot file on the boot server. The filename can include a pathname.

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** boot-server (DHCP)

## boot-server

See the following sections:



### *boot-server (DHCP)*

**Syntax** boot-server *address*;

**Hierarchy Level** [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup.

**Options** *address*—Address of a boot server. You must specify an IPv4 address, not a hostname.

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** boot-file

## *boot-server (NTP)*

**Syntax** boot-server *address*;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the server that NTP queries when the router boots to determine the local date and time.

When you boot the router, it issues an ntpdate request, which polls a network server to determine the local date and time. You need to configure a server that the router uses to determine the time when the router boots. Otherwise, NTP will not be able to synchronize to a time server if the server's time appears to be very far off of the local router's time.

**Options** *address*—Address of an NTP server. You must specify an address, not a hostname.

**Usage Guidelines** See "Configuring the NTP Boot Server" on page 101.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## broadcast

**Syntax** broadcast *address* <key *key-number*> <version *value*> <ttl *value*>;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the local router to operate in broadcast mode with the remote system at the specified *address*. In this mode, the local router sends periodic broadcast messages to a client population at the specified broadcast or multicast *address*. Normally, you include this statement only when the local router is operating as a transmitter.

**Options** *address*—The broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be 224.0.1.1.

key *key-number*—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.
**Range:** Any unsigned 32-bit integer

*value*—(Optional) Time-to-live (TTL) value to use.
**Range:** 1 through 255
**Default:** 1

version *value*—(Optional) Specify the version number to be used in outgoing NTP packets.
**Range:** 1 through 4
**Default:** 4

**Usage Guidelines** See "Configuring the NTP Time Server and Time Services" on page 102.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## broadcast-client

**Syntax** broadcast-client;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the local router to listen for broadcast messages on the local network to discover other servers on the same subnet.

**Usage Guidelines** See "Configuring the Router to Listen for Broadcast Messages" on page 105.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## bucket-size

**Syntax** bucket-size *bucket-size*;

**Hierarchy Level** [edit system internet-options icmpv4-rate-limit],
[edit system internet-options icmpv6-rate-limit]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** The number of seconds in the rate limiting bucket.

**Options** bucket-size
**Range:** 0 through 4294967295 seconds
**Default:** 5

**Usage Guidelines** See "Configuring the ICMP4 Rate Limit" on page 199 and "Configuring the ICMPv6 Rate Limit" on page 199.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## change-type

**Syntax** change-type (character-sets | set-transitions);

**Hierarchy Level** [edit system login password]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Set requirements for using character sets in plain-text passwords. When combined with the minimum-changes statement, you can check for the total number of character sets included in the password or for the total number of character set changes in the password. Newly created passwords must meet these requirements.

**Options** One of the following:

- character-sets—The number of character sets in the password. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.
- set-transitions—The number of transitions between character sets.

**Usage Guidelines** See "Configuring Special Requirements for Plain-Text Passwords" on page 55.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** minimum-changes

## circuit-type

**Syntax** circuit-type;

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify that the circuit type is concatenated with the username during the subscriber authentication process.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## class

See the following sections:



### *class (Assign a Class to an Individual User)*

**Syntax** class *class-name*;

**Hierarchy Level** [edit system login user *username*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a user's login class. You must configure one class for each user.

**Options** *class-name*—One of the classes defined at the [edit system login class] hierarchy level.

**Usage Guidelines** See "Configuring User Accounts" on page 72.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *class (Define Login Classes)*

**Syntax**
```
class class-name {
   allow-commands "regular-expression";
   allow-configuration "regular-expression";
   deny-commands "regular-expression";
   deny-configuration "regular-expression";
   idle-timeout minutes;
   no-world-readable;
   permissions [ permissions ];
}
```

**Hierarchy Level** [edit system login]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define login classes.

**Options** *class-name*—A name you choose for the login class.

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See "Defining Login Classes" on page 61.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** user

## client-identifier

**Syntax** client-identifier (ascii *client-id* | hexadecimal *client-id*);

**Hierarchy Level** [edit system services dhcp static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Configure the client's unique identifier. This identifier is used by the DHCP server to index its database of address bindings. Either a client identifier or the client's MAC address is required to uniquely identify the client on the network.

**Options** *client-id*—A name or number that uniquely identifies the client on the network. The client identifier can be an ASCII string or hexadecimal digits.

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## commit

**Syntax**

```
commit {
    allow-transients;
    file filename.xsl {
        optional;
        refresh;
        refresh-from url;
        source url;
    }
    refresh;
    refresh-from url;
    source url;
    traceoptions {
        file filename <files number> <size size>;
        flag flag;
    }
}
```

**Hierarchy Level** [edit system scripts]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For JUNOS commit scripts, configure commit-time scripting mechanism.

The statements are explained separately.

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

## commit synchronize

**Syntax** commit synchronize;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For multiple Routing Engines only. Configure a commit command to automatically result in a commit synchronize. The Routing Engine on which you execute the commit command (requesting Routing Engine) copies and loads its candidate configuration to the other (responding) Routing Engines. All Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on all Routing Engines.

**Usage Guidelines** See "Configuring Multiple Routing Engines to Synchronize Configurations Automatically" on page 58.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## compress-configuration-files

**Syntax** (compress-configuration-files | no-compress-configuration-files);

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Compress the current operational configuration file. By default, the current operational configuration file is compressed, and is stored in the file juniper.conf, in the /config file system, along with the last three committed versions of the configuration. However, with large networks, the current configuration file might exceed the available space in the /config file system. Compressing the current configuration file allows the file to fit in the file system, typically reducing the size of the file by 90 percent. The current configuration file is compressed on the second commit of the configuration after the first commit is made to include the compress-configuration-files statement.

**NOTE:** We recommend that you enable compression of the router configuration files to minimize the amount of disk space that they require.

**Default** The current operational configuration file is uncompressed.

**Usage Guidelines** See “Compressing the Current Configuration File” on page 58.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## configuration

**Syntax**

```
configuration {
    transfer-interval interval;
    transfer-on-commit;
    archive-sites {
        ftp://<username>:<password>@<host>:<port>/<url-path>;
    }
}
```

**Hierarchy Level** [edit system archival]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the router to transfer its currently active configuration by means of FTP periodically or after each commit. The remaining statements are explained separately.

**Usage Guidelines** See "Configuring a Router to Transfer Its Configuration to an Archive Site" on page 192.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** transfer-interval, transfer-on-commit, and archive.

## configuration-servers

**Syntax**

```
configuration-servers {
    url;
}
```

**Hierarchy Level** [edit system autoinstallation]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only, configure the URL address of a server from which to obtain configuration files. Examples of URLs:

tftp://tftpconfig.sp.com/config.conf;

ftp://user:password:@sftpconfig.sp.com/path file-name/

**Usage Guidelines** See the Getting Started Guide for your router model.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** autoinstallation, idle-timeout.

## connection-limit

**Syntax** connection-limit *limit*;

**Hierarchy Level** [edit system services finger],
[edit system services ftp],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the maximum number of established connections for each type of system service.

**Options** *limit*—(Optional) Maximum number of established connections.
**Range:** 1 through 250
**Default:** 75

**Usage Guidelines** See "Configuring System Services" on page 145.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## console

See the following sections:

- console (Physical Port) on page 263
- console (System Logging) on page 264

### *console (Physical Port)*

**Syntax**

```
console {
    insecure;
    log-out-on-disconnect;
    type terminal-type;
    disable;
}
```

**Hierarchy Level** [edit system ports]

**Release Information** Statement introduced before JUNOS Release 7.4.
disable option added in JUNOS Release 7.6.

**Description** Configure the characteristics of the console port, which is on the router's craft interface.

**Default** The console port is enabled and its speed is 9600 baud.

**Options**

insecure—Disable root login connections to the console and auxiliary ports. Configuring the console port as insecure also prevents superusers and anyone with a user identifier (UID) of 0 from establishing terminal connections in multiuser mode.

log-out-on-disconnect—Log out the session when the data carrier on the console port is lost.

type *terminal-type*—Type of terminal that is connected to the port.
**Range:** ansi, vt100, small-xterm, xterm
**Default:** The terminal type is unknown, and the user is prompted for the terminal type.

disable—Disable console login connections.

**Usage Guidelines** See "Configuring Console and Auxiliary Port Properties" on page 142.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

### *console (System Logging)*

**Syntax**
```
console {
    facility severity;
}
```

**Hierarchy Level** [edit system syslog]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the logging of system messages to the system console.

**Options** *facility*—Class of messages to log. To specify multiple classes, include multiple *facility severity* statements. For a list of the facilities, see Table 19 on page 115.

*severity*—Severity of the messages that belong to the facility specified by the paired *facility* name. Messages with severities the specified level and higher are logged. For a list of the severities, see Table 20 on page 116.

**Usage Guidelines** See "Directing Messages to the Console" on page 118.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS System Log Messages Reference*

## default-address-selection

**Syntax** default-address-selection;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Use the loopback interface, lo0, as the source address for all locally generated IP packets. The lo0 interface is the interface to the router's Routing Engine.

**Default** The outgoing interface is used as the source address.

**Usage Guidelines** See "Configuring the Source Address for Locally Generated TCP/IP Packets" on page 143 and the *JUNOS Network Interfaces Configuration Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## default-lease-time

**Syntax** default-lease-time *seconds*;

**Hierarchy Level** [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Specify the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server. This setting is used if a lease time is not requested by the client.

**Options** *seconds*—Number of seconds the lease can be held.
**Default:** 86400 (1 day)

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** maximum-lease-time

## delimiter

**Syntax** delimiter *delimiter-character*;

**Hierarchy Level**
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify the character used as the delimiter between the concatenated components of the username. The semicolon (;) cannot be used as a delimiter.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## deny-commands

**Syntax** deny-commands "*regular-expression*";

**Hierarchy Level** [edit system login class]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify the operational mode commands that the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.

**Default** If you omit this statement and the allow-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.

**Options** *regular-expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

**Usage Guidelines** See "Specifying Operational Mode Commands" on page 65.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** allow-commands, user

## deny-configuration

**Syntax** deny-configuration "*regular-expression*";

**Hierarchy Level** [edit system login class]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify the configuration mode commands that the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.

**Default** If you omit this statement and the allow-configuration statement, users can issue only those commands for which they have access privileges through the permissions statement.

**Options** *regular-expression*—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

**Usage Guidelines** See "Specifying Operational Mode Commands" on page 65.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** allow-configuration, user

## destination

**Syntax**

```
destination {
    radius {
        server {
            server-address {
                accounting-port port-number;
                secret password;
                source-address address;
                retry number;
                timeout seconds;
            }
        }
    }
    tacplus {
        server {
            server-address {
                secret password;
                single-connection;
                timeout seconds;
                port port-number;
            }
        }
    }
}
```

**Hierarchy Level** [edit system accounting]

**Release Information** Statement introduced before JUNOS Release 7.4.
radius statement added in JUNOS Release 7.4.

**Description** Configure the authentication server.

**Options** The remaining statements are explained separately.

**Usage Guidelines** See "Configuring RADIUS System Accounting" on page 194 and "Configuring TACACS+ System Accounting" on page 197.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## destination-override

**Syntax**
```
destination-override {
    syslog host ip-address ;
}
```

**Hierarchy Level** [edit system tracing]

**Release Information** Statement introduced in JUNOS Release 9.2.

**Description** This option overrides the system-wide configuration under [edit system tracing] and has no effect if system tracing is not configured.

**Options**
- syslog—Specify the system process log files to send to the remote tracing host.
- host *ip-address*—Specify the host and IP address to send tracing information.

**Usage Guidelines** See "Tracing and Logging Operations" on page 38.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** tracing

## dhcp

**Syntax**

```
dhcp {
    boot-file filename;
    boot-server (address | hostname);
    domain-name domain-name;
    domain-search [domain-list];
    default-lease-time seconds;
    maximum-lease-time seconds;
    name-server {
        address;
    }
    option {
        [ (id-number option-type option-value) | (id-number array option-type option-value) ];
    }
    pool address/prefix-length {
        address-range {
            low address;
            high address;
        }
        exclude-address {
            address;
        }
    }
    router {
        address;
    }
    static-binding mac-address {
        fixed-address {
            address;
        }
        host hostname;
        client-identifier (ascii client-id | hexadecimal client-id);
    }
    server-identifier address;
    wins-server {
        address;
    }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Configure a router or interface as a DHCP server. A DHCP server can allocate network addresses and deliver configuration information to client hosts on a TCP/IP network.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring a DHCP Server” on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## dhcp-local-server

**Syntax**

```
dhcp-local-server {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    interface interface-name <upto upto-interface-name> <exclude>;
    }
    pool-match-order {
        ip-address-first;
        option-82 (Extended DHCP Local Server);
    }
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable><match
            regex>;
        flag flag;
    }
}
```

**Hierarchy Level**

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services],
[edit logical-systems *logical-system-name* system services],
[edit routing-instances *routing-instance-name* system services],
[edit system services]

**Release Information**

Statement introduced in JUNOS Release 9.0.

**Description** Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router and enable the router to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The DHCP local server interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication. You can configure authentication support on a global basis or for a specific group of interfaces.

The DHCP local server also supports the use of JUNOS software address-assignment pools or external authorities, such as RADIUS, to provide the client address and configuration information.

The extended DHCP local server is incompatible with the J-series DHCP server and is not supported on the J-series Services Router. Also, the DHCP local server and the DHCP/BOOTP relay, which are configured under the [edit forwarding-options helpers] hierarchy level, cannot both be enabled on the router at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

**NOTE:** When you configure the dhcp-local-server statement at the routing instance hierarchy level, you must use a routing instance type of virtual-router.

The statements are explained separately.

**Usage Guidelines** See “Configuring the Extended DHCP Local Server” on page 165.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** address-assignment, dhcp-attributes

## diag-port-authentication

**Syntax** diag-port-authentication (encrypted-password "*password*" | plain-text-password);

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a password for performing diagnostics on the router's System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), or Forwarding Engine Board (FEB) port.

For routers that have more than one SSB, the same password is used for both SSBs.

**NOTE:** Do not run diagnostics on the SCB, SSB, SFM, or FEB unless you have been instructed to do so by Customer Support personnel.

**Default** No password is configured on the diagnostics port.

**Options** encrypted-password *password*—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password for each user.

**Usage Guidelines** See "Configuring the Password on the Diagnostics Port" on page 190.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## domain-name

See the following sections:

- domain-name (DHCP) on page 276
- domain-name (Subscriber Access Management) on page 277
- domain-name (Router) on page 277

### *domain-name (DHCP)*

**Syntax** domain-name *domain-name*;

**Hierarchy Level** [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.

**Options** *domain-name*—Name of the domain.

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *domain-name (Subscriber Access Management)*

**Syntax** domain-name *domain-name-string*;

**Hierarchy Level**
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify the domain name that is concatenated with the username during the subscriber authentication process.

**Options** *domain-name-string*—The domain name formatted string.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *domain-name (Router)*

**Syntax** domain-name *domain-name*;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the name of the domain in which the router is located. This is the default domain name that is appended to hostnames that are not fully qualified.

**Options** *domain-name*—Name of the domain.

**Usage Guidelines** See “Configuring the Router’s Domain Name” on page 49.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## domain-search

**Syntax** domain-search [ *domain-list* ];

**Hierarchy Level** [edit system],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-bindings]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a list of domains to be searched.

**Options** *domain-list*—A list of domain names to search. The list can contain up to 6 domain names, with a total of up to 256 characters.

**Usage Guidelines** See "Configuring Which Domains to Search" on page 49 and "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## dump-device

**Syntax**

```
dump-device {
    compact-flash;
    removable-compact-flash;
    usb;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Configure the medium used for storing memory snapshots of system failure. When you specify the storage and an operating system fails, the operating system writes a snapshot of the state of the router when it failed to the storage medium. When the operating system is rebooted, the storage device is checked for a snapshot. If found, the snapshot of memory is written to the /var/crash directory on the router and can be examined by Juniper Networks customer support to help determine the cause of failure.

If the swap partition on the device medium is not large enough for the system memory snapshot, the snapshot is not successfully written to the directory. Use the request system snapshot command to specify the swap partition.

**Options** compact-flash—The primary CompactFlash card.

removable-compact-flash—The CompactFlash card on the front of the router (J4300 and J6300 only) as the system software failure memory snapshot device.

usb—The device attached to the universal serial bus (USB) port.

**Usage Guidelines** See the Getting Started Guide for your router model.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## events

**Syntax** events [*events* ];

**Hierarchy Level** [edit system accounting]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the types of events to track and log.

**Options** *events*—Event types; can be one or more of the following:

- login—Audit logins.
- change-log—Audit configuration changes.
- interactive-commands—Audit interactive commands (any command-line input).

**Usage Guidelines** See "Specifying Events" on page 197.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## explicit-priority

**Syntax** explicit-priority;

**Hierarchy Level** [edit system syslog file *filename*],
[edit system syslog host]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Record the priority (facility and severity level) in each standard-format system log message directed to a file or remote destination.

When the structured-data statement is also included at the [edit system syslog file *filename*] hierarchy level, this statement is ignored for the file.

**Usage Guidelines** See "Including Priority Information in System Log Messages" on page 125.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** structured-data, *JUNOS System Log Messages Reference*

## facility-override

**Syntax** facility-override *facility*;

**Hierarchy Level** [edit system syslog host]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Substitute an alternate facility for the default facilities used when messages are directed to a remote destination.

**Options** *facility*—Alternate facility to substitute for the default facilities. For a list of the possible facilities, see Table 22 on page 121.

**Usage Guidelines** See "Changing the Alternative Facility Name for Remote Messages" on page 120.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS System Log Messages Reference*

# file

See the following sections:

- file (Commit Scripts) on page 282
- file (System Logging) on page 283

## *file (Commit Scripts)*

**Syntax**

```
file filename.xsl {
    optional;
    refresh;
    refresh-from url;
    source url;
}
```

**Hierarchy Level** [edit system scripts commit]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For JUNOS commit scripts, enable a commit script that is located in the /var/db/scripts/commit directory.

**Options** *filename*—The name of an XSLT file containing a commit script.

The statements are explained separately.

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

## *file (System Logging)*

**Syntax**

```
file filename {
    facility severity;
    explicit-priority;
    match "regular-expression";
    structured-data {
        brief;
    }
    archive {
        files number;
        size size;
        (world-readable | no-world-readable);
    }
}
```

**Hierarchy Level** [edit system syslog]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the logging of system messages to a file.

**Options** *facility*—Class of messages to log. To specify multiple classes, include multiple *facility severity* statements. For a list of the facilities, see Table 19 on page 115.

*filename*—File in the /var/log directory in which to log messages from the specified facility. To log messages to more than one file, include more than one file statement.

*severity*—Severity of the messages that belong to the facility specified by the paired *facility* name. Messages with severities the specified level and higher are logged. For a list of the severities, see Table 20 on page 116.

The remaining statements are explained separately.

**Usage Guidelines** See "Directing Messages to a Log File" on page 116.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS System Log Messages Reference*

## files

**Syntax** files *number*;

**Hierarchy Level** [edit system syslog archive],
[edit system syslog file *filename* archive]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the maximum number of archived log files to retain. When the JUNOS logging utility has written a defined maximum amount of data to a log file *logfile*, it closes the file, compresses it, and renames it to *logfile*.0.gz (for information about the maximum file size, see size). The utility then opens and writes to a new file called *logfile*. When the new file reaches the maximum size, the *logfile*.0.gz file is renamed to *logfile*.1.gz, and the new file is closed, compressed, and renamed *logfile*.0.gz. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).

**Options** *number*—Maximum number of archived files.
**Range:** 1 through 1000
**Default:** 10 files

**Usage Guidelines** See "Specifying Log File Size, Number, and Archiving Properties" on page 123.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** size, *JUNOS System Log Messages Reference*

## finger

**Syntax**
```
finger {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Allow finger requests from remote systems to the local router.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring Finger Service" on page 180.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## flow-tap-dtcp

**Syntax**

```
flow-tap-dtcp {
   ssh {
      connection-limit limit;
      rate-limit limit;
   }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in JUNOS Release 8.1.

**Description** Configure Digital Transmission Content Protection (DTCP) sessions to run over SSH in support of the flow-tap application.

**Options**

connection-limit *limit*—(Optional) Maximum number of connections allowed.
**Range:** 1 through 250
**Default:** 75

rate-limit *limit*—(Optional) Maximum number of connection attempts allowed per minute.
**Range:** 1 through 250
**Default:** 150

**Usage Guidelines** See "Configuring DTCP-over-SSH Service for the Flow-Tap Application" on page 179.

**Required Privilege Level** flow-tap—To view this statement in the configuration.
flow-tap-control—To add this statement to the configuration.

## format

**Syntax** format (md5 | sha1 | des);

**Hierarchy Level** [edit system login passwords]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure the authentication algorithm for plain-text passwords.

**Default** For JUNOS software, the default encryption format is md5. For JUNOS-FIPS software, the default encryption format is sha1.

**Options** The hash algorithm that authenticates the password can be one of three algorithms:

- md5—Produces a 128-bit digest.
- sha1—Produces a 160-bit digest.
- des—Has a block size of 8 bytes; its key size is 48 bits long.

**Usage Guidelines** See "Configuring Special Requirements for Plain-Text Passwords" on page 55.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ftp

**Syntax**
```
ftp {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Allow FTP requests from remote systems to the local router.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring FTP Service" on page 180.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## full-name

**Syntax** full-name *complete-name*;

**Hierarchy Level** [edit system login user]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the complete name of a user.

**Options** *complete-name*—Full name of the user. If the name contains spaces, enclose it in quotation marks.

**Usage Guidelines** See "Configuring User Accounts" on page 72.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## gre-path-mtu-discovery

**Syntax** (gre-path-mtu-discovery | no-gre-path-mtu-discovery);

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure path MTU discovery for outgoing GRE tunnel connections:

- gre-path-mtu-discovery—Path MTU discovery is enabled.
- no-gre-path-mtu-discovery—Path MTU discovery is disabled.

**Default** Path MTU discovery is disabled.

**Usage Guidelines** See "Configuring GRE Path MTU Discovery" on page 201.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## group

**Syntax**

```
group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    interface interface-name <upto upto-interface-name> <exclude>;
}
```

**Hierarchy Level**

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* system services dhcp-local-server],
[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

**Release Information**

Statement introduced in JUNOS Release 9.0.

**Description**

Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.

**Options**

*group-name*—Name of the group.

**Usage Guidelines**

See "Configuring the Extended DHCP Local Server" on page 165 and "Using External AAA Authentication Services" on page 170.

**Required Privilege Level**

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## host

**Syntax**

```
host (hostname | other-routing-engine| scc-master) {
   facility severity;
   explicit-priority;
   facility-override facility;
   log-prefix string;
   match "regular-expression";
}
```

**Hierarchy Level** [edit system syslog]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the logging of system messages to a remote destination.

**Options**

*facility*—Class of messages to log. To specify multiple classes, include multiple *facility severity* statements. For a list of the facilities, see Table 19 on page 115.

*hostname*—IPv4 address, IPv6 address, or fully qualified hostname of the remote machine to which to direct messages. To direct messages to multiple remote machines, include a host statement for each one.

*severity*—Severity of the messages that belong to the facility specified by the paired *facility* name. Messages with severities the specified level and higher are logged. For a list of the severities, see Table 20 on page 116.

other-routing-engine—Direct messages to the other Routing Engine on a routing platform with two Routing Engines installed and operational.

scc-master—On a T640 routing node that is part of a routing matrix, direct messages to the TX Matrix platform.

The remaining statements are explained separately.

**Usage Guidelines** See "Directing Messages to a Remote Machine or the Other Routing Engine" on page 118 and "Directing Messages to a Remote Destination from the Routing Matrix" on page 138.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS System Log Messages Reference*

## host-name

**Syntax** host-name *hostname*;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Set the hostname of the router.

**Options** *hostname*—Name of the router.

**Usage Guidelines** See "Configuring the Router's Name and Addresses" on page 47.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## http

**Syntax**
```
http {
    interfaces [ interface-names ];
    port port;
}
```

**Hierarchy Level** [edit system services web-management]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure port and interfaces for HTTP service, which is unencrypted.

**Options** interfaces [ *interface-names* ]—Name of one or more interfaces on which to allow the HTTP service. By default, HTTP access is allowed through built-in Fast Ethernet interfaces only.

The remaining statement is explained separately in this chapter.

**Usage Guidelines** See the *J-Web Interface User Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** https, port (HTTP/HTTPS), web-management

## https

**Syntax**

```
https {
    interfaces [ interface-names ];
    local-certificate name;
    port port;
}
```

**Hierarchy Level** [edit system services web-management]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the secure version of HTTP (HTTPS) service, which is encrypted.

**Options**

interfaces [ *interface-names* ]— Name of one or more interfaces on which to allow the HTTPS service. By default, HTTPS access is allowed through any ingress interface, but HTTP access is allowed through built-in Fast Ethernet interfaces only.

local-certificate *name*— Name of the X.509 certificate for a secure sockets layer (SSL) connection. An SSL connection is configured at the [edit security certificates local] hierarchy.

The remaining statement is explained separately.

**Usage Guidelines** See the *J-Web Interface User Guide*.

**Required Privilege Level**

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** http, port (HTTP/HTTPS), web-management

## icmpv4-rate-limit

**Syntax**
```
icmpv4-rate-limit {
    bucket-size bucket-size;
    packet-rate packet-rate;
}
```

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure rate limiting parameters for ICMPv4 messages sent.

**Options** The remaining statements are explained separately.

**Usage Guidelines** See “Configuring the ICMP4 Rate Limit” on page 199.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## icmpv6-rate-limit

**Syntax**
```
icmpv6-rate-limit {
    bucket-size bucket-size;
    packet-rate packet-rate;
}
```

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure rate limiting parameters for ICMPv6 messages sent.

**Options** The remaining statements are explained separately.

**Usage Guidelines** See “Configuring the ICMPv6 Rate Limit” on page 199.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## idle-timeout

**Syntax** idle-timeout *minutes*;

**Hierarchy Level** [edit system login class *class-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For a login class, configure the maximum time that a session can be idle before the user is logged off the router. The session times out after remaining at the CLI operational mode prompt for the specified time.

**Default** If you omit this statement, a user is never forced off the system after extended idle times.

**Options** *minutes*—Maximum idle time.
**Range:** 0 through 100,000 minutes

**Usage Guidelines** See "Configuring the Timeout Value for Idle Login Sessions" on page 71.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** user

## inet6-backup-router

**Syntax** inet6-backup-router *address* <destination *destination-address*>;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Set a default router (running IP version 6 [IPv6]) to use while the local router (running IPv6) is booting and if the routing protocol processes fail to start. The JUNOS software removes the route to this router as soon as the software starts.

**Options** *address*—Address of the default router.

destination *destination-address*—(Optional) Destination address that is reachable through the backup router. Include this option to achieve network reachability while loading, configuring, and recovering the router, but without the risk of installing a default route in the forwarding table.
**Default:** All hosts (default route) are reachable through the backup router.

**Usage Guidelines** See "Configuring a Backup Router" on page 50.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## interface

See the following sections:



### *interface (ARP Aging Timer)*

**Syntax** interface *interface-name minutes*;

**Hierarchy Level** [edit system arp aging-timer]

**Release Information** Statement introduced in JUNOS Release 9.4.

**Description** Specify the ARP aging timer in minutes for a logical interface of family type inet.

**Options** *minutes*—Time between ARP updates, in minutes.
**Default:** 20
**Range:** 1 through 240

**Usage Guidelines** See "Adjusting the ARP Aging Timer" on page 204.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *interface (DHCP Local Server)*

**Syntax** interface *interface-name* <upto *upto-interface-name*> <exclude>;

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
[edit system services dhcp-local-server group *group-name*]

**Release Information** Statement introduced in JUNOS Release 9.0.
upto and exclude options introduced in JUNOS Release 9.1.

**Description** Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface *interface-name* statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.

**Options** exclude—Exclude an interface or a range of interfaces from the group.

*inteface-name*—Name of the interface. You can repeat this keyword multiple times.

upto *upto-interface-name*—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the *upto-interface-name* must be the same as the device name of the *interface-name*.

**Usage Guidelines** See "Configuring the Extended DHCP Local Server" on page 165 and "Using External AAA Authentication Services" on page 170.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## interfaces

**Syntax**

```
interfaces {
    interface-name {
        bootp;
        rarp;
        slarp;
    }
}
```

**Hierarchy Level** [edit system autoinstallation]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Configure the interface on which to perform autoinstallation. A request for an IP address is sent from the interface. Specify the IP address procurement protocol.

**Options** bootp

rarp—Send requests over Ethernet interfaces.

slarp—Send requests over serial interfaces.

**Usage Guidelines** See the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** autoinstallation

## internet-options

**Syntax**

```
internet-options {
    tcp-mss mss-value;
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit {
        bucket-size bucket-size;
        packet-rate packet-rate;
    }
    icmpv6-rate-limit {
        bucket-size bucket-size;
        packet-rate packet-rate;
    }
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    ipv6-duplicate-addr-detection-transmits;
    (ipv6-reject-zero-hop-limit | no-ipv6-reject-zero-hop-limit);
    (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout;
    no-tcp-rfc1323;
    no-tcp-rfc1323-paws;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit <upper-limit>;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure system Internet Protocol options to protect against certain types of DoS attacks.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the ICMP4 Rate Limit" on page 199, "Configuring the ICMPv6 Rate Limit" on page 199, "Configuring IP-IP Path MTU Discovery" on page 200, "Configuring GRE Path MTU Discovery" on page 201, "Configuring Path MTU Discovery" on page 202, "Configuring IPv6 Duplicate Address Detection Transmits" on page 201, "Configuring Acceptance of IPv6 Packets with Zero Hop-Limit" on page 201, "Configuring Source Quench" on page 202, "Configuring the Router to Drop Packets with the SYN and FIN Bits Set" on page 202, "Configuring No TCP RFC 1323 Extensions" on page 203, "Configuring No TCP RFC 1323 PAWS Extension" on page 203, "Configuring the Range of Port Addresses" on page 203, and "Configuring TCP MSS for Session Negotiation" on page 200.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ip-address-first

**Syntax** ip-address-first;

**Hierarchy Level** [edit logical-systems *logical-system-name* system services dhcp-local-server pool-match-order],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the giaddr if one is present in the DHCP client PDU. If no giaddr is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.

**Usage Guidelines** See "Configuring the Extended DHCP Local Server" on page 165.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ipip-path-mtu-discovery

**Syntax** (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure path MTU discovery for outgoing IP-IP tunnel connections:

- ipip-path-mtu-discovery—Path MTU discovery is enabled.
- no-ipip-path-mtu-discovery—Path MTU discovery is disabled.

**Default** Path MTU discovery is disabled.

**Usage Guidelines** See "Configuring IP-IP Path MTU Discovery" on page 200.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ipv6-duplicate-addr-detection-transmits

**Syntax** ipv6-duplicate-addr-detection-transmits;

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Control the number of attempts for IPv6 duplicate address detection.

**Default** The default value is 3.

**Usage Guidelines** See "Configuring IPv6 Duplicate Address Detection Transmits" on page 201.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ipv6-path-mtu-discovery

**Syntax** (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced in JUNOS Release 9.2.

**Description** Configure path MTU discovery for IPv6 packets.

**Default** IPv6 path MTU discovery is enabled.

**Options** ipv6-path-mtu-discovery—IPv6 path MTU discovery is enabled.

no-ipv6-path-mtu-discovery—IPv6 path MTU discovery is disabled.

**Usage Guidelines** See "Configuring IPv6 Path MTU Discovery" on page 201.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ipv6-path-mtu-discovery-timeout

**Syntax** ipv6-path-mtu-discovery-timeout *minutes*;

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced in JUNOS Release 9.2.

**Description** Set IPv6 path MTU discovery timeout interval.

**Default** The default timeout is 10 minutes.

**Usage Guidelines** See "Configuring IPv6 Path MTU Discovery" on page 201.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ipv6-reject-zero-hop-limit

**Syntax** (ipv6-reject-zero-hop-limit | no-ipv6-reject-zero-hop-limit);

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Enable and disable rejecting incoming ipv6 packets with zero hop limit in their header.

**Usage Guidelines** See "Configuring Acceptance of IPv6 Packets with Zero Hop-Limit" on page 201.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** See no-ipv6-reject-zero-hop-limit.

## limits

**Syntax**
```
limits {
   active-child-process [ process-limit ];
}
```

**Hierarchy Level** [edit system services web-management]

**Release Information** Statement introduced in JUNOS Release 8.3.

**Description** Configure limits on the number of simultaneous HTTPD child processes that can be started to prevent DOS attacks on the HTTP port.

**Options** active-child-process [ *process-limit* ]—Maximum number of simultaneous HTTPD child processes that can be started.
**Range:** 0 through 32
**Default:** 5

**Usage Guidelines** See the *J-Web Interface User Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## load-key-file

**Syntax**
```
load-key-file;
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Load RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys from a file. The file is a URL containing one or more SSH keys.

**Usage Guidelines** See "Configuring the Root Password" on page 53 and "Configuring User Accounts" on page 72.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## local-certificate

**Syntax** local-certificate;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Import or reference a SSL certificate.

**Usage Guidelines** See “Configuring SSL Service for JUNOScript Client Applications” on page 146 and “Importing SSL Certificates for JUNOScript Support” on page 587.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## location

**Syntax**

```
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the system location in various formats.

**Options**

altitude *feet*—Number of feet above sea level.

building *name*—Name of building. The name of the building can be 1 to 28 characters in length. If the string contains spaces, enclose it in quotation marks (" ").

country-code *code*—Two-letter country code.

floor *number*—Floor in the building.

hcoord *horizontal-coordinate*—Bellcore Horizontal Coordinate.

lata *service-area*—Long-distance service area.

latitude *degrees*—Latitude in degree format.

longitude *degrees*—Longitude in degree format.

npa-nxx *number*—First six digits of the phone number (area code and exchange).

postal-code *postal-code*—Postal code.

rack *number*—Rack number.

vcoord *vertical-coordinate*—Bellcore Vertical Coordinate.

**Usage Guidelines** See "Configuring the System Location" on page 52.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## log-prefix

**Syntax** log-prefix *string*;

**Hierarchy Level** [edit system syslog host]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Include a text string in each message directed to a remote destination.

**Options** *string*—Text string to include in each message.

**Usage Guidelines** See "Adding a Text String to System Log Messages" on page 122.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS System Log Messages Reference*

## logical-system-name

**Syntax** logical-system-name;

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify that the logical system name is concatenated with the username during the subscriber authentication process. No logical system name is concatenated if the configuration is in the default logical system.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## login

**Syntax**

```
login {
    announcement text;
    class class-name {
        allow-commands "regular-expression";
        allow-configuration "regular-expression";
        deny-commands "regular-expression";
        deny-configuration "regular-expression";
        idle-timeout minutes;
        login-tip;
        permissions [ permissions ];
    }
    message text;
    password {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication authentication;
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure user access to the router.

**Options** The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Configuring User Access” on page 61.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## login-alarms

**Syntax** login-alarms;

**Hierarchy Level** [edit system login class admin]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Show system alarms automatically when an admin user logs on to the router.

**Usage Guidelines** See "Configuring System Alarms to Appear Automatically" on page 205.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** *J-series Services Router Administration Guide*

## login-tip

**Syntax** login-tip;

**Hierarchy Level** [edit system login class *class-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Enable CLI tips at login.

**Default** Disabled.

**Usage Guidelines** See "Configuring Tips" on page 72.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## mac-address

**Syntax** mac-address;

**Hierarchy Level**
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify that the MAC address from the client PDU is concatenated with the username during the subscriber authentication process.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## match

**Syntax** match "*regular-expression*";

**Hierarchy Level** [edit system syslog file *filename*],
[edit system syslog host *hostname* | other-routing-engine| scc-master)],
[edit system syslog user (*username* | *)]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify a text string that must (or must not) appear in a message for the message to be logged to a destination.

**Usage Guidelines** See "Using Regular Expressions to Refine the Set of Logged Messages" on page 128.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## max-configurations-on-flash

**Syntax** max-configurations-on-flash *number*;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify the number of configurations stored on the CompactFlash card.

**Options** *number*—The number of configurations stored on the CompactFlash card.
**Range:** 0 through 49. The most recently saved configuration is number 0, and the oldest saved configuration is number 49.

**Usage Guidelines** See "Specifying the Number of Configurations Stored on the CompactFlash Card" on page 194.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration

## maximum-lease-time

**Syntax** maximum-lease-time *seconds*;

**Hierarchy Level** [edit system services dhcp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

Exception: Dynamic BOOTP lease length can exceed the maximum lease length specified.

**Options** *seconds*—The maximum number of seconds the lease can be held.

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration

**Related Topics** default-lease-time

## maximum-length

**Syntax** maximum-length *length*;

**Hierarchy Level** [edit system login passwords]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Specify the maximum number of characters allowed in plain-text passwords. Newly created passwords must meet this requirement.

**Default** For JUNOS-FIPS software, the maximum number of characters for plain-text passwords is 20. For JUNOS software, no maximum is set.

**Options** length—The maximum number of characters the password can include.
**Range:** 1 to 64 characters

**Usage Guidelines** See "Configuring Special Requirements for Plain-Text Passwords" on page 55.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## message

**Syntax** message *text*;

**Hierarchy Level** [edit system login]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a system login message. This message appears before a user logs in.

**Options** *text*—Text of the message.

**Usage Guidelines** See "Configuring a System Login Message" on page 187.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration

**Related Topics** announcement

## minimum-changes

**Syntax** minimum-changes *number*;

**Hierarchy Level** [edit system login passwords]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Specify the minimum number of character sets (or character set changes) required in plain-text passwords. Newly created passwords must meet this requirement.

This statement is used in combination with the change-type statement. If the change-type is character-sets, then the number of character sets included in the password is checked against the specified minimum. If change-type is set-transitions, then the number of character set changes in the password is checked against the specified minimum.

**Default** For JUNOS software, the minimum number of changes is 1. For JUNOS-FIPS software, the minimum number of changes is 3.

**Options** *number*—The minimum number of character sets (or character set changes) required for the password.

**Usage Guidelines** See "Configuring Special Requirements for Plain-Text Passwords" on page 55.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** change-type

## minimum-length

**Syntax** minimum-length *length*;

**Hierarchy Level** [edit system login passwords]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Specify the minimum number of characters required in plain-text passwords. Newly created passwords must meet this requirement.

**Default** For JUNOS software, the minimum number of characters for plain-text passwords is six. For JUNOS-FIPS software, the minimum number of characters for plain-text passwords is 10.

**Options** length—The minimum number of characters the password must include.
**Range:** 6 to 20 characters

**Usage Guidelines** See "Configuring Special Requirements for Plain-Text Passwords" on page 55.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** maximum-length

## mirror-flash-on-disk

**Syntax** mirror-flash-on-disk;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the hard disk to automatically mirror the contents of the CompactFlash card. The hard disk maintains a synchronized mirror copy of the CompactFlash card contents. Data written to the CompactFlash card is simultaneously updated in the mirrored copy of the hard disk. If the CompactFlash card fails to read data, the hard disk automatically retrieves its mirrored copy of the CompactFlash card. This command is not available on the J-series routers.

**CAUTION:** We recommend that you disable flash disk mirroring when you upgrade or downgrade the router.

You cannot issue the request system snapshot command while the mirror-flash-on-disk statement is enabled.

**NOTE:** After you have enabled or disabled the mirror-flash-on-disk statement, you must reboot the router for your changes to take effect. To reboot, issue the request system reboot command.

**Usage Guidelines** See “Configuring Flash Disk Mirroring” on page 52.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## multicast-client

**Syntax** multicast-client <*address*>;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For NTP, configure the local router to listen for multicast messages on the local network to discover other servers on the same subnet.

**Options** *address*—(Optional) One or more IP addresses. If you specify addresses, the router joins those multicast groups.
**Default:** 224.0.1.1.

**Usage Guidelines** See "Configuring the Router to Listen for Multicast Messages" on page 106.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## name-server

**Syntax**
```
name-server {
   address;
}
```

**Hierarchy Level** [edit system],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure one or more Domain Name System (DNS) name servers.

**Options** *address*—Address of the name server. To configure multiple name servers, include multiple *address* options.

**Usage Guidelines** See "Configuring a DNS Name Server" on page 50 and "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## no-compress-configuration-files

**See** compress-configuration-files.

## no-gre-path-mtu-discovery

**See** gre-path-mtu-discovery.

## no-ipip-path-mtu-discovery

**See** ipip-path-mtu-discovery.

## no-ipv6-reject-zero-hop-limit

**See** ipv6-reject-zero-hop-limit.

## no-multicast-echo

**Syntax** no-multicast-echo;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in JUNOS Release 8.1

**Description** Disable the Routing Engine from responding to ICMP echo requests sent to multicast group addresses.

**Default** The Routing Engine responds to ICMP echo requests sent to multicast group addresses.

**Usage Guidelines** See "Disabling the Response to Multicast Ping Packets" on page 144.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## no-path-mtu-discovery

**See** path-mtu-discovery.

## no-ping-record-route

**Syntax** no-ping-record-route;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in JUNOS Release 9.4.

**Description** Disable the reporting of the IP address in the ICMP echo responses.

**Usage Guidelines** See “Disabling the Reporting of IP Address and Timestamps in Ping Responses” on page 144.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## no-ping-time-stamp

**Syntax** no-ping-time-stamp;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in JUNOS Release 9.4.

**Description** Disable the reporting of timestamps in the ICMP echo responses.

**Usage Guidelines** See “Disabling the Reporting of IP Address and Timestamps in Ping Responses” on page 144.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## no-redirects

**Syntax** no-redirects;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Disable the sending of protocol redirect messages by the router.

To disable the sending of redirect messages on a per-interface basis, include the no-redirects statement at the [edit interfaces *interface-name* unit *logical-unit-number* family *family*] hierarchy level.

**Default** The router sends redirect messages.

**Usage Guidelines** See "Disabling the Sending of Redirect Messages on the Router" on page 143.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS Network Interfaces Configuration Guide*

## no-remote-trace

**See** tracing.

## no-saved-core-context

**See** saved-core-context.

## no-source-quench

**See** source-quench.

## no-tcp-rfc1323

**Syntax** no-tcp-rfc1323;

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the JUNOS software to disable RFC 1323 TCP extensions.

**Usage Guidelines** See “Configuring No TCP RFC 1323 Extensions” on page 203.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## no-tcp-rfc1323-paws

**Syntax** no-tcp-rfc1323-paws;

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the JUNOS software to disable the RFC 1323 Protection Against Wrapped Sequence (PAWS) number extension.

**Usage Guidelines** See “Configuring No TCP RFC 1323 PAWS Extension” on page 203.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## no-world-readable

**See** world-readable.

## ntp

**Syntax**

```
ntp {
    authentication-key number type type value password;
    boot-server (NTP) address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    server address <key key-number> <version value> <prefer>;
    source-address source-address;
    trusted-key [ key-numbers ];
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure NTP on the router.

**Options** The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Configuring the Network Time Protocol” on page 100.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## option-60

**Syntax** option-60;

**Hierarchy Level**
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU is concatenated with the username during the subscriber authentication process.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## option-82

See the following sections:

- option-82 (Extended DHCP Local Server) on page 321
- option-82 (Subscriber Access Management) on page 322

### *option-82 (Extended DHCP Local Server)*

**Syntax** option-82;

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit logical-systems *logical-system-name* system services dhcp-local-server pool-match-order],
[edit routing-instances *routing-instance-name* system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the ip-address-first statement before configuring the option-82 statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool.

**Usage Guidelines** See "Configuring the Extended DHCP Local Server" on page 165.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *option-82 (Subscriber Access Management)*

**Syntax** option-82 <circuit-id> <remote-id>;

**Hierarchy Level**
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify the type of option 82 information from the client PDU that is concatenated with the username during the subscriber authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption be supplied, the raw payload of option 82 from the PDU is concatenated to the username.

**Options** circuit-id—The string for the Agent Circuit ID suboption (suboption 1).

remote-id—The string for the Agent Remote ID suboption (suboption 2).

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## optional

**Syntax** optional;

**Hierarchy Level** [edit system scripts commit file *filename*]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For JUNOS commit scripts, allow a commit operation to succeed even if the script specified in the file statement is missing from the /var/db/scripts/commit directory on the routing platform. The optional statement allows the commit operation to progress as if the commit script were not enabled in the configuration.

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

## outbound-ssh

**Syntax**

```
[edit system services]
outbound-ssh {
   client client-id {
      address {
         port port-number;
         retry number;
         timeout seconds;
      }
      device-id device-id;
      keep-alive {
         retry number;
         timeout seconds;
      }
      reconnect-strategy (in-order | sticky);
      secret password;
      services netconf;
   }
   traceoptions {
      file <filename> <files number> <match regular-expression> <size maximum-file-size>
         <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
   }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in JUNOS Release 8.4.

**Description** Configure a router running the JUNOS software behind a firewall to communicate with client management applications on the other side of the firewall.

**Default** To configure transmission of the router's device ID to the application, include the device-id statement at the [edit system services] hierarchy level.

**Options**

client-id—Identifies the outbound-ssh configuration stanza on the router. Each outbound-ssh stanza represents a single outbound SSH connection. This attribute is not sent to the client.

device-id—Identifies the router to the client during the initiation sequence.

secret—(Optional) Specifies the JUNOS router's public SSH host key. If added to the outbound-ssh statement, during the initialization of the outbound SSH service, the router passes its public key to the management server. This is the recommended method of maintaining a current copy of the router's public key.

keep-alive—(Optional) When configured, specifies that the router send keepalive messages to the management server. To configure the keepalive message, you must set both the timeout and retry attributes.

retry—Specifies the number of keepalive messages the router sends without receiving a response from the client before the current SSH connection will be disconnected. The default is three messages.

timeout—Specifies the amount of time that the JUNOS server waits for data before sending a keep alive signal. The default is 15 seconds.

reconnect-strategy—(Optional) Specifies the method the JUNOS router uses to reestablish a disconnected outbound SSH connection. Two methods available:

- sticky—Specifies that the router attempt to reconnect to the management server that it was last connected with first. If the connection is unavailable, it attempts to establish a connection with the next client on the list and so forth until a connection is made.
- in-order—Specifies that the router attempt to establish an outbound SSH session based on the management server address list. The router attempts to establish a session with the first server on the list. If this connection is not available, the router attempts to establish a session with the next server, and so on down the list until a connection is established.

When reconnecting to a client, the router attempts to reconnect to the client based on the retry and timeout values for each client listed.

services—Specifies the services available for the session. Currently, NETCONF is the only service available.

address—Indicates the hostname or the IPv4 address of the NSM application server. You can list multiple clients by adding each client's IP address or hostname along with the following connection parameters:

- port—Sets the outbound SSH port for the client. The default is port 22.
- retry—Specifies the number of times the JUNOS router will attempt to establish an outbound SSH connection before giving up. The default is 3 tries.
- timeout—Sets the amount of time that the router attempts to establish an outbound SSH connection before giving up. The default is 15 seconds.

filename—(Optional) By default, the file name of the log file used to record the trace options is the name of traced process (for example mib2d or snmpd). Use this option to override the default value.

files—(Optional) The maximum number of trace files generated. By default, the maximum number of trace files is 10. Use this option to override the default value.

When a trace file reaches its maximum size, the system archives the file and starts a new file. The system archives trace files by appending a number to the file name in sequential order from 1 to the maximum value (specified by the default value or the options value set here). Once the maximum value is reached, the numbering sequence is restarted at 1, overwriting the older file.

size—(Optional) The maximum size of the trace file in kilobytes (KB). Once the maximum file size is reached, the system archives the file. The default value is 1000 KB. Use this option to override the default value.

match—(Optional) When used, the system only adds lines to the trace file that match the the regular expression specified. For example, if the match value is set to =error, the system only records lines to the trace file that include the string error.

world-readable | no-world-readable—(Optional) This option specifies whether the files are accessible by the originator of the trace operation only or by any user. By default, log files are only accessible by the user that started the trace operation (no-world-readable).

all | configuration | connectivity—(Optional) This flag specifies the type of tracing operation to perform.

all—Log all events.

configuration—Log all events pertaining to the configuration of the router.

connectivity—Log all events pertaining to the establishment of a connection between the client server and the router.

no-remote-trace—(Optional) Disables remote tracing.

**Usage Guidelines** See "Configuring Outbound SSH Service" on page 182.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## packet-rate

**Syntax** packet-rate *packet-rate*;

**Hierarchy Level** [edit system internet-options icmpv4-rate-limit],
[edit system internet-options icmpv6-rate-limit]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** The rate-limiting packets earned per second.

**Options** *packet-rate*
**Range:** 0 through 4294967295 seconds
**Default:** 1000

**Usage Guidelines** See "Configuring the ICMPv6 Rate Limit" on page 199 and "Configuring the ICMP4 Rate Limit" on page 199.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## password

See the following sections:



### *password (Login)*

**Syntax**

```
password {
   change-type (set-transitions | character-set);
   format (md5 | sha1 | des);
   maximum-length length;
   minimum-changes number;
   minimum-length length;
}
```

**Hierarchy Level** [edit system login]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.

**Options** The remaining statements are explained separately in this chapter.

**Usage Guidelines** See "Configuring Special Requirements for Plain-Text Passwords" on page 55.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** maximum-length.

## *password (Subscriber Access Management)*

**Syntax** password *password-string*;

**Hierarchy Level**
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server group *group-name* authentication]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the password that is sent to the external AAA authentication server for subscriber authentication.

**Options** *password-string*—Authentication password.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## path-mtu-discovery

**Syntax** (path-mtu-discovery | no-path-mtu-discovery);

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure path MTU discovery for outgoing Transmission Control Protocol (TCP) connections:

- path-mtu-discovery—Path MTU discovery is enabled.
- no-path-mtu-discovery—Path MTU discovery is disabled.

**Default** Path MTU discovery is disabled.

**Usage Guidelines** See “Configuring Path MTU Discovery” on page 202.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## peer

**Syntax** peer *address* <key *key-number*> <version *value*> <prefer>;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For NTP, configure the local router to operate in symmetric active mode with the remote system at the specified address. In this mode, the local router and the remote system can synchronize with each other. This configuration is useful in a network in which either the local router or the remote system might be a better source of time.

**Options** *address*—Address of the remote system. You must specify an address, not a hostname.

key *key-number*—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.
**Range:** Any unsigned 32-bit integer

prefer—(Optional) Mark the remote system as the preferred host, which means that if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

version *value*—(Optional) Specify the NTP version number to be used in outgoing NTP packets.
**Range:** 1 through 4
**Default:** 4

**Usage Guidelines** See "Configuring the NTP Time Server and Time Services" on page 102.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## permissions

**Syntax** permissions [ *permissions* ];

**Hierarchy Level** [edit system login class]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the login access privileges to be provided on the router.

**Options** *permissions*—Privilege type. For a list of permission flag types, see Table 11 on page 63.

**Usage Guidelines** See "Configuring Access Privilege Levels" on page 62.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** user

## pic-console-authentication

**Syntax**
```
pic-console authentication {
   (encrypted-password "password" | plain-text-password);
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure console access to Physical Interface Cards (PICs).

**Default** Disabled. By default, there is no password setting for console access.

**Options** encrypted-password " *password*"—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.

The default requirements for plain-text passwords are:

- The password must be between 6 and 128 characters long
  - You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
  - Valid passwords must contain at least one change of case or character class.

**Usage Guidelines** See "Configuring Console Access to PICs" on page 187.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** Configuring Console and Auxiliary Port Properties on page 142.

## pool

**Syntax**

```
pool address/prefix-length {
    address-range {
        low address;
        high address;
    }
    exclude-address {
        address;
    }
}
```

**Hierarchy Level** [edit system services dhcp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool.

**Options**

address-range—Lowest and highest IP addresses in the pool that are available for dynamic address assignment. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

exclude-address—Addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range.

**Usage Guidelines** See “Configuring a DHCP Server” on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## pool-match-order

**Syntax**

```
pool-match-order {
    ip-address-first;
    option-82 (Extended DHCP Local Server);
}
```

**Hierarchy Level**

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* system services dhcp-local-server],
[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

**Release Information**

Statement introduced in JUNOS Release 9.0.

**Description**

Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client. By default, the DHCP local server uses the ip-address-first method to determine which address pool to use.

The statements are explained separately.

**Usage Guidelines**

See "Configuring the Extended DHCP Local Server" on page 165.

**Required Privilege Level**

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## port

See the following sections:

- port (HTTP/HTTPS) on page 335
- port (RADIUS Server) on page 335
- port (SRC Server) on page 336
- port (TACACS+ Server) on page 336

### *port (HTTP/HTTPS)*

**Syntax** port *port-number*;

**Hierarchy Level** [edit system services web-management]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the port on which the HTTP or HTTPS service is connected.

**Options** *port*—The TCP port number on which the specified service listens.

**Usage Guidelines** See the *J-Web Interface User Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** web-management, http, https

### *port (RADIUS Server)*

**Syntax** port *port-number*;

**Hierarchy Level** [edit system radius-server *address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the port number on which to contact the RADIUS server.

**Options** *number*—Port number on which to contact the RADIUS server.
**Default:** 1812 (as specified in RFC 2865)

**Usage Guidelines** See "Configuring RADIUS Authentication" on page 77.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *port (SRC Server)*

**Syntax** port *port-number*;

**Hierarchy Level** [edit system services service-deployment servers *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the port number on which to contact the SRC server.

**Options** *port-number*—(Optional) The TCP port number for the SRC server.
**Default:** 3333

**Usage Guidelines** See "Enabling the SRC Software" on page 199.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *port (TACACS+ Server)*

**Syntax** port *port-number*;

**Hierarchy Level** [edit system accounting destination tacplus server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the port number on which to contact the TACACS+ server.

**Options** *number*—Port number on which to contact the TACACS+ server.
**Default:** 49

**Usage Guidelines** See "Configuring TACACS+ System Accounting" on page 197.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ports

**Syntax**

```
ports {
    auxiliary {
        type terminal-type;
    }
    console {
        type terminal-type;
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the properties of the console and auxiliary ports, which are located on the router's craft interface.

**Options** The remaining statements are explained separately in this chapter.

**Usage Guidelines** See "Configuring Console and Auxiliary Port Properties" on page 142.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## processes

**Syntax**

```
processes {
    process-name (enable | disable) failover (alternate-media | other-routing-engine);
    timeout seconds;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure which JUNOS software processes are running on the router.

**CAUTION:** Never disable any of the software processes unless instructed to do so by a customer support engineer.

**Default** All processes are enabled by default.

**Options** (enable | disable)—(Optional) Enables or disables a specified process.

failover (alternate-media | other-routing-engine)—(Optional) For routers with redundant Routing Engines only, switch to backup media if a process fails repeatedly. If a process fails four times within 30 seconds, the router reboots from the alternate media or the other Routing Engine.

*process-name*—One of the valid process names. You can obtain a complete list of process names by using the CLI command completion feature. After specifying a process name, command completion also indicates any additional options for that process.

timeout *seconds*—(Optional) How often the system checks the watchdog timer, in seconds. If the watchdog timer has not been checked in the specified number of seconds, the system reloads. If you set the time value too low, it is possible for the system to reboot immediately after it loads.
**Range:** 15, 60, 180
**Default:** 180 seconds (rounded up to 291 seconds by the JUNOS kernel)

**Usage Guidelines** See “Disabling JUNOS Software Processes” on page 189.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## protocol-version

**Syntax** protocol-version *version*;

**Hierarchy Level** [edit system services ssh]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify the secure shell (SSH) protocol version.

**Options** *version*—v1, v2, or [ v1 v2 ]
**Default:** v2

**Usage Guidelines** See "Configuring the SSH Protocol Version" on page 182.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## radius

**Syntax**
```
radius {
    server {
        server-address {
            accounting-port port-number;
            secret password;
            source-address address;
            retry number;
            timeout seconds;
        }
    }
}
```

**Hierarchy Level** [edit system accounting destination]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure the RADIUS accounting server.

**Options** *server-address*—Address of the RADIUS accounting server.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring RADIUS System Accounting" on page 194.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## radius-options

**Syntax**

```
radius-options {
   attributes {
      nas-ip-address ip-address;
   }
   password-protocol mschap-v2;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in JUNOS Release 8.3.
MS-CHAPv2 password protocol configuration option introduced in JUNOS Release 9.2.

**Description** Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

**Options** *ip-address*—IP address of the network access server (NAS) that requests user authentication.

*mschap-v2*—Protocol MS-CHAPv2, used for password authentication and password changing.

**Usage Guidelines** See “Configuring MS-CHAPv2 for Password-Change Support” on page 80.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## radius-server

**Syntax**

```
radius-server server-address {
    accounting-port port-number;
    port number;
    retry number;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a RADIUS server for Point-to-Point Protocol (PPP).

To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

**Options** *server-address*—Address of the RADIUS authentication server.

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Configuring RADIUS Authentication” on page 77.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## rate-limit

**Syntax** rate-limit *limit*;

**Hierarchy Level** [edit system services finger],
[edit system services ftp],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Maximum number of connection attempts on an access service.

**Options** rate-limit *limit*—(Optional) Maximum number of connection attempts allowed per minute.
**Range:** 1 through 250
**Default:** 150

**Usage Guidelines** See "Configuring System Services" on page 145.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## refresh

**Syntax** refresh;

**Hierarchy Level** [edit system scripts commit],
[edit system scripts commit file *filename*]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For JUNOS commit scripts, overwrite the local copy of all enabled commit scripts or a single enabled script located in the /var/db/scripts/commit directory with the copy located at the source URL, as specified in the source statement.

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

**Related Topics** refresh-from, source

## refresh-from

**Syntax** refresh-from *url*;

**Hierarchy Level** [edit system scripts commit],
[edit system scripts commit file *filename*]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For JUNOS commit scripts, overwrite the local copy of all enabled commit scripts or a single enabled script located in the /var/db/scripts/commit directory with the copy located at a URL other than the URL specified in the source statement.

**Options** *url*—The source specified as an HTTP URL, FTP URL, or SCP-style remote file specification.

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

**Related Topics** refresh, source

## retry

**Syntax** retry *number*;

**Hierarchy Level** [edit system radius-server *server-address*],
[edit system accounting destination radius server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Number of times the router is allowed to try to contact a RADIUS authentication or accounting server.

**Options** *number*—Number of retries allowed for contacting a RADIUS server.
**Range:** 1 through 10
**Default:** 3

**Usage Guidelines** See "Configuring RADIUS Authentication" on page 77 and "Configuring RADIUS System Accounting" on page 194.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** timeout

## retry-options

**Syntax**

```
retry-options {
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
    tries-before-disconnect number;
}
```

**Hierarchy Level** [edit system login]

**Release Information** Statement introduced in JUNOS Release 8.0.

**Description** Maximum number of times a user can attempt to enter a password while logging in through SSH or Telnet before being disconnected.

**Options**

backoff-threshold *number*—Threshold for the number of failed login attempts before the user experiences a delay when attempting to reenter a password. Use the backoff-factor option to specify the length of delay, in seconds.
**Range:** 1 through 3
**Default:** 2

backoff-factor *seconds*—Length of delay after each failed login attempt. The length of delay increases by this value for each subsequent login attempt after the value specified in the backoff-threshold option.
**Range:** 5 through 10
**Default:** 5

minimum-time *seconds*—Minimum length of time that the connection remains open while the user is attempting to enter a password to log in.
**Range:** 20 through 60
**Default:** 20

tries-before-disconnect *number*—Maximum number of times a user is allowed to attempt to enter a password to log in through SSH or Telnet.
**Range:** 1 through 10
**Default:** 10

**Usage Guidelines** See "Limiting the Number of Login Attempts for SSH and Telnet Sessions" on page 75.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** rate-limit

## root-authentication

**Syntax**

```
root-authentication {
    (encrypted-password "password" | plain-text-password);
    ssh-dsa "public-key";
    ssh-rsa "public-key";
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the authentication methods for the root-level user, whose username is root.

**Options** encrypted-password "*password*"—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.

You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.

ssh-dsa "*public-key*"—SSH version 2 authentication. Specify the DSA (SSH version 2) public key. You can specify one or more public keys.

ssh-rsa "*public-key*"—SSH version 1 authentication. Specify the RSA (SSH version 1 and SSH version 2) public key. You can specify one or more public keys.

**Usage Guidelines** See "Configuring the Root Password" on page 53.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** authentication (Login)

## root-login

**Syntax** root-login (allow | deny | deny-password);

**Hierarchy Level** [edit system services ssh]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Control user access through SSH.

**Options** allow—Allow users to log in to the router as root through SSH.
**Default:** allow

deny—Disable users from logging in to the router as root through SSH.

deny-password—Allow users to log in to the router as root through SSH when the authentication method (for example, RSA authentication) does not require a password.

**Usage Guidelines** See "Configuring the Root Login" on page 181.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** Configuring SSH Service on page 181.

## router

**Syntax**
```
router {
  address;
}
```

**Hierarchy Level** [edit system services dhcp-service],
[edit system services dhcp-service pool],
[edit system services dhcp-service static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Specify IPv4 addresses for one or more routers available to a DHCP client. List routers in order of preference.

**Options** address—IPv4 address of the router. To configure multiple routers, include multiple address options.

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## routing-instance-name

**Syntax** routing-instance-name;

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify that the routing instance name is concatenated with the username during the subscriber authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## saved-core-context

**Syntax** (saved-core-context | no-saved-core-context);

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure whether the router saves core files generated by internal JUNOS processes, along with contextual information (system log files and a copy of the current configuration):

- saved-core-context—The router saves each cores file and its associated context in a compressed tar file named /var/tmp/*process-name*.core.*core-number*.tgz.
- no-saved-core-context—The router does not save cores files and their associated context.

The router saves core files.

**Usage Guidelines** See "Saving Core Files from JUNOS Processes" on page 190.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** saved-core-files

## saved-core-files

**Syntax** saved-core-files *number*;

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Save core files generated by internal JUNOS processes, but not the associated contextual information (configuration and system log files).

**Options** *number*—Maximum number of core files to save.
**Range:** 1 through 64

**Usage Guidelines** See "Saving Core Files from JUNOS Processes" on page 190.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** saved-core-context

## scripts

**Syntax**

```
scripts {
    commit {
        file filename.xsl {
            optional;
            refresh;
            refresh-from url;
            source url;
        }
        traceoptions {
            file filename <files number> <size size>;
            flag flag;
        }
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For JUNOS commit scripts, configure scripting mechanisms.

The statements are explained separately.

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

## secret

**Syntax** secret *password*;

**Hierarchy Level** [edit system accounting destination radius server *server-address*],
[edit system accounting destination tacplus server *server-address*],
[edit system radius-server *server-address*],
[edit system tacplus-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the password to use with the RADIUS or TACACS+ server. The secret password used by the local router must match that used by the server.

**Options** *password*—Password to use; can include spaces included in quotation marks.

**Usage Guidelines** See "Configuring RADIUS Authentication" on page 77, "Configuring TACACS+ Authentication" on page 81, "Configuring TACACS+ System Accounting" on page 197, and "Configuring RADIUS System Accounting" on page 194.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## server

See the following sections:

- server (NTP) on page 351
- server (RADIUS Accounting) on page 352
- server (TACACS+ Accounting) on page 352

### *server (NTP)*

**Syntax** server *address* <key *key-number*> <version *value*> <prefer>;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For NTP, configure the local router to operate in client mode with the remote system at the specified *address*. In this mode, the local router can be synchronized with the remote system, but the remote system can never be synchronized with the local router.

**Options** *address*—Address of the remote system. You must specify an address, not a hostname.

key *key-number*—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.
**Range:** Any unsigned 32-bit integer

prefer—(Optional) Mark the remote system as preferred host, which means that if all other things are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

version *value*—(Optional) Specify the version number to be used in outgoing NTP packets.
**Range:** 1 through 4
**Default:** 4

**Usage Guidelines** See "Configuring the NTP Time Server and Time Services" on page 102.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *server (RADIUS Accounting)*

**Syntax**
```
server {
    server-address {
        accounting-port port-number;
        secret password;
        source-address address;
        retry number
        timeout seconds;
    }
}
```

**Hierarchy Level** [edit system accounting destination radius]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure RADIUS logging.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring RADIUS System Accounting" on page 194.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *server (TACACS+ Accounting)*

**Syntax**
```
server {
    server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
    }
}
```

**Hierarchy Level** [edit system accounting destination tacplus]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure TACACS+ logging.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring TACACS+ System Accounting" on page 197.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## server-identifier

**Syntax** server-identifier *address*;

**Hierarchy Level** [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Configure a server identifier. This is an optional setting that can be used to identify a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).

Servers include the server identifier in DHCPOFFER messages so that clients can distinguish between multiple lease offers. Clients include the server identifier in DHCPREQUEST messages to select a lease and indicate which offer is accepted from multiple lease offers. Also, clients can use the server identifier to send unicast request messages to specific DHCP servers to renew a current lease.

This address must be a manually assigned, static IP address. The server cannot send a request and receive an IP address from itself or another DHCP server.

**Default** If no server identifier is set, the DHCP server sets the server identifier based on the primary interface address used by the server to receive a client request. For example, if the client sends a DHCP request and the server receives it on fe-0/0/0 and the primary interface address is 1.1.1.1, then the server identifier is set to 1.1.1.1.

**Options** *address*—The IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## servers

**Syntax**
```
servers server-address {
    port port-number;
}
```

**Hierarchy Level** [edit system services service-deployment]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure an IPv4 address for the Session and Resource Control (SRC) server.

**Options** *server-address*—The TCP port number.
**Default:** 3333

The remaining statement is explained separately in this chapter.

**Usage Guidelines** See “Enabling the SRC Software” on page 199.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## service-deployment

**Syntax**
```
service-deployment {
    servers server-address {
        port port-number;
    }
    source-address source-address;
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Enable JUNOS software to work with the SRC software.

**Options** The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Enabling the SRC Software” on page 199.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## services

**Syntax**

```
services {
    dhcp {
        dhcp_services;
    }
    finger {
        <connection-limit limit>;
        <rate-limit limit>;
    }
    ftp {
        <connection-limit limit>;
        <rate-limit limit>;
    }
    ssh {
        root-login (allow | deny | deny-password);
        protocol-version [v1 v2];
        <connection-limit limit>;
        <rate-limit limit >;
    }
    service-deployment {
        servers server-address {
            port-number port-number;
        }
        source-address source-address;
    }
    telnet {
        <connection-limit limit>;
        <rate-limit limit>;
    }
    web-management {
        http {
            interfaces [ interface-names ];
            port port;
        }
        https {
            interfaces [ interface-names ];
            local-certificate name;
            port port;
        }
        limits {
            active-child-process [ process-limit ];
        }
        session {
            idle-timeout [ minutes ];
            session-limit [ session-limit ];
        }
    }
    xnm-clear-text {
        <connection-limit limit>;
        <rate-limit limit>;
    }
    xnm-ssl {
```

```
        <connection-limit limit>;
        <rate-limit limit>;
        <local-certificate name>
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the router so that users on remote systems can access the local router through the DHCP server, finger, rlogin, SSH, telnet, Web management, JUNOScript clear-text, JUNOScript SSL, and network utilities or enable JUNOS software to work with the SRC software.

The statements are explained separately.

**Usage Guidelines** See "Configuring System Services" on page 145 and "Enabling the SRC Software" on page 199.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## session

**Syntax**

```
session {
    idle-timeout [ minutes ];
    session-limit [ session-limit ];
}
```

**Hierarchy Level** [edit system services web-management]

**Release Information** Statement introduced in JUNOS Release 8.3.

**Description** Configure limits for the number of minutes a session can be idle before it times out, and configure the number of simultaneous J-Web user login sessions.

**Options**

idle-timeout *minutes*—Configure the number of minutes a session can be idle before it times out.
**Range:** 1 through 1440
**Default:** 1440

session-limit *session-limit*—Configure the maximum number of simultaneous J-Web user login sessions.
**Range:** 1 through 1024
**Default:** Unlimited

**Usage Guidelines** See the *J-Web Interface User Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## single-connection

**Syntax** single-connection;

**Hierarchy Level** [edit system tacplus-server *server-address*],
[edit system accounting destination tacplus-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt.

**Usage Guidelines** See "Configuring TACACS+ Authentication" on page 81 and "Configuring TACACS+ System Accounting" on page 197.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## size

**Syntax** size *size*;

**Hierarchy Level** [edit system syslog archive],
[edit system syslog file *filename* archive]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the maximum amount of data that the JUNOS logging utility writes to a log file *logfile* before archiving it (closing it, compressing it, and changing its name to *logfile*.0.gz). The utility then opens and writes to a new file called *logfile*. For information about the number of archive files that the utility creates in this way, see files.

**Options** *size*—Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).
**Syntax:** *x*k to specify the number of kilobytes, *x*m for the number of megabytes, or *x*g for the number of gigabytes
**Range:** 64 KB through 1 GB
**Default:** 128 KB for J-series Services Routers; 1 MB for M-series, MX-series, and T-series routing platforms; 10 MB for TX Matrix platforms

**Usage Guidelines** See "Specifying Log File Size, Number, and Archiving Properties" on page 123.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** files, *JUNOS System Log Messages Reference*

## source

**Syntax** source *url*;

**Hierarchy Level** [edit system scripts commit],
[edit system scripts commit file *filename*]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** For JUNOS commit scripts, specify the location of the source file for all enabled commit scripts or a single enabled script located in the /var/db/scripts/commit directory. When you include the refresh statement, the source URL is the location from which the local copy is refreshed.

**Options** *url*—The source specified as an HTTP URL, FTP URL, or SCP-style remote file specification.

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

**Related Topics** refresh, refresh-from

## source-address

See the following sections:



### *source-address (NTP, RADIUS, System Logging, or TACACS+)*

**Syntax** source-address *source-address*;

**Hierarchy Level** [edit system accounting destination radius server *server-address*],
[edit system accounting destination tacplus server *server-address*],
[edit system ntp],
[edit system radius-server *server-address*],
[edit system syslog],
[edit system tacplus-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify a source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine.

**Options** *source-address*—A valid IP address configured on one of the router interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all host *hostname* statements at the [edit system syslog] hierarchy level, but not for messages directed to the other Routing Engine or to the TX Matrix platform in a routing matrix.

**Usage Guidelines** See "Specifying a Source Address for RADIUS and TACACS+ Servers" on page 84, "Specifying a Source Address for an NTP Server" on page 101, and "Specifying an Alternative Source Address for System Log Messages" on page 119.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

### *source-address (SRC Software)*

**Syntax** source-address *source-address*;

**Hierarchy Level** [edit system services service-deployment]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Enable JUNOS software to work with the SRC software.

**Options** *source-address*—(Optional) The local IPv4 address to be used as source address for traffic to the SRC server. The source address restricts traffic within the out-of-band network.

**Usage Guidelines** See "Enabling the SRC Software" on page 199.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## source-port

**Syntax** source-port upper-limit <*upper-limit*>;

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the range of port addresses.

**Options** upper-limit *upper-limit*—(Optional) The range of port addresses and can be a value from 5000 through 65,355.

**Usage Guidelines** See "Configuring the Range of Port Addresses" on page 203.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## source-quench

**Syntax** (source-quench | no-source-quench);

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure how the JUNOS software handles Internet Control Message Protocol (ICMP) source quench messages:

- source-quench—The JUNOS software ignores ICMP source quench messages.
- no-source-quench—The JUNOS software does not ignore ICMP source quench messages.

**Default** The JUNOS software does not ignore ICMP source quench messages.

**Usage Guidelines** See "Configuring Source Quench" on page 202.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ssh

**Syntax**
```
ssh {
    root-login (allow | deny | deny-password);
    protocol-version [v1 v2];
    <connection-limit limit>;
    <rate-limit limit>;
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Allow SSH requests from remote systems to the local router.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring SSH Service" on page 181.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## start-time

**Syntax** start-time *date.time*;

**Hierarchy Level** [edit system syslog file *filename* archive]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** Specify the date and time for a one-time transfer of a system logging archive file to a remote archiving site.

**Options** *date.time*—Date and time at which you want the log file transfer to begin. The format for this value is yyyy-mm-dd.hh:mm.

**Usage Guidelines** See "Specifying Log File Size, Number, and Archiving Properties" on page 123.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## static-binding

**Syntax**

```
static-binding mac-address {
    fixed-address {
        address;
    }
    host client-hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
}
```

**Hierarchy Level** [edit system services dhcp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address or client identifier.

**Options**

*mac-address*—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.

fixed-address *address*—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

host *client-hostname*—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the domain-name statement.

client-identifier (ascii *client-id* | hexadecimal *client-id*)—Used by the DHCP server to index the database of address bindings. The client identifier is an ASCII string or hexadecimal number and can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## static-host-mapping

**Syntax**

```
static-host-mapping {
    hostname {
        inet [ address ];
        sysid system-identifier;
        alias [ alias ];
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Map a hostname to one or more IP addresses and aliases, and configure an International Organization for Standardization (ISO) system identifier (system ID).

**Options**

alias *alias*—(Optional) Alias for the hostname.

*hostname*—Fully qualified hostname.

inet *address*—IP address. You can specify one or more IP addresses for the host.

sysid *system-identifier*—ISO system identifier (system ID). This is the 6-byte portion of the Intermediate System-to-Intermediate System (IS-IS) network service access point (NSAP). We recommend that you use the host's IP address represented in binary-coded decimal (BCD) format. For example, the IP address 208.197.169.18 is 2081.9716.9018 in BCD.

**Usage Guidelines** See "Configuring the Router's Name and Addresses" on page 47.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## structured-data

**Syntax**
```
structured-data {
    brief;
}
```

**Hierarchy Level** [edit system syslog file *filename*]

**Release Information** Statement introduced in JUNOS Release 8.3.

**Description** Write system log messages to the log file in structured-data format, which complies with Internet draft draft-ietf-syslog-protocol-21.txt, *The syslog Protocol* (http://www.ietf.org/internet-drafts/draft-ietf-syslog-protocol-21.txt).

**NOTE:** When this statement is included, other statements that specify the format for messages written to the file are ignored (the explicit-priority statement at the [edit system syslog file *filename*] hierarchy level and the time-format statement at the [edit system syslog] hierarchy level.

**Usage Guidelines** See "Logging Messages in Structured-Data Format" on page 117.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** explicit-priority, time-format, *JUNOS System Log Messages Reference*

## syslog

**Syntax**

```
syslog {
    archive {
        files number;
        size size;
        (world-readable | no-world-readable);
    }
    console {
        facility severity;
    }
    file filename {
        facility severity;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
        archive {
            archive-sites {
                site-name;
            }
            files number;
            size size;
            start-time date.time;
            transfer-interval interval;
            (world-readable | no-world-readable);
        }
    }
    host (hostname | other-routing-engine | scc-master) {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string;
        match "regular-expression";
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the types of system log messages to log to files, a remote destination, user terminals, or the system console.

The statements are explained separately.

**Usage Guidelines** See "Configuring System Log Messages" on page 109.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS System Log Messages Reference*

## system

**Syntax**
```
system { ... }
```

**Hierarchy Level** [edit]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure system management properties.

**Usage Guidelines** See "System Management Configuration Statements" on page 41.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## tacplus

**Syntax**
```
tacplus {
    server {
        server-address {
            port port-number;
            secret password;
            single-connection;
            timeout seconds;
        }
    }
}
```

**Hierarchy Level** [edit system accounting destination]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the Terminal Access Controller Access Control System Plus (TACACS+).

**Options** *server-address*—Address of the TACACS+ authentication server.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring TACACS+ System Accounting" on page 197.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## tacplus-options

**Syntax**

```
tacplus-options {
    service-name service-name;
    (no-cmd-attribute-value | exclude-cmd-attribute);
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.
The no-cmd-attribute-value and exclude-cmd-attribute option introduced in JUNOS Release 8.5.

**Description** Configure TACACS+ options for authentication and accounting.

**Options**

service-name *service-name*—The name of the authentication service used when configuring multiple TACACS+ servers to use the same authentication service.
**Default:** junos-exec

no-cmd-attribute-value—Set the cmd attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.

exclude-cmd-attribute—Exclude the cmd attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.

**Usage Guidelines** See "Configuring the Same Authentication Service for Multiple TACACS+ Servers" on page 85 and "Configuring TACACS+ Accounting" on page 197.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## tacplus-server

**Syntax**
```
tacplus-server server-address {
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the TACACS+ server.

**Options** *server-address*—Address of the TACACS+ authentication server.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring TACACS+ Authentication" on page 81.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## tcp-drop-synfin-set

**Syntax**
```
tcp-drop-synfin-set;
```

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the router to drop packets that have both the SYN and FIN bits set.

**Usage Guidelines** See "Configuring the Router to Drop Packets with the SYN and FIN Bits Set" on page 202.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## tcp-mss

**Syntax** tcp-mss *mss-value*;

**Hierarchy Level** [edit system internet-options]

**Release Information** Statement introduced in JUNOS Release 9.2 of J-series Services Routers software.

**Description** (J-series Services Routers only) Enable and specify the TCP maximum segment size (TCP MSS) to be used to replace that of TCP SYN packets whose MSS option is set to a higher value than the value you choose.

If the router receives a TCP packet with the SYN bit and MSS option set and the MSS option specified in the packet is larger than the MSS specified by the tcp-mss command, the router replaces the MSS value in the packet with the lower value specified by the tcp-mss statement.

This statement enables you to specify the MSS size in TCP SYN packets used during session establishment. Decreasing the MSS size helps to limit packet fragmentation and to protect against packet loss that can occur when a packet must be fragmented to meet the MTU size but the packet's DF (don't fragment) bit is set.

Use the tcp-mss statement to specify a lower TCP MSS value than the value in the TCP SYN packets.

**Options** *mss-value*—TCP MSS value for SYN packets with a higher MSS value set.
**Range:** 64 through 65535 seconds
**Default:** TCP MSS is disabled.

**Usage Guidelines** See "Configuring TCP MSS for Session Negotiation" on page 200.

For more information about the TCP MSS statement and session negotiation, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## telnet

**Syntax**

```
telnet {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Allow Telnet connections from remote systems to the local router.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring System Services" on page 145.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## time-format

**Syntax** time-format (year | millisecond | year millisecond);

**Hierarchy Level** [edit system syslog]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Include the year, the millisecond, or both, in the timestamp on every standard-format system log message. The additional information is included for messages directed to each destination configured by a file, console, or user statement at the [edit system syslog] hierarchy level, but not to destinations configured by a host statement.

By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged, for example, Aug 21 12:36:30.

**NOTE:** When the structured-data statement is included at the [edit system syslog file *filename*] hierarchy level, this statement is ignored for the file.

**Options** millisecond—Include the millisecond in the timestamp.

year—Include the year in the timestamp.

**Usage Guidelines** See "Including the Year or Millisecond in Timestamps" on page 127.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** structured-data, *JUNOS System Log Messages Reference*

## timeout

**Syntax** timeout *seconds*;

**Hierarchy Level** [edit system radius-server *server-address*],
[edit system tacplus-server *server-address*],
[edit system accounting destination radius server server-address],
[edit system accounting destination tacplus server server-address]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the amount of time that the local router waits to receive a response from a RADIUS or TACACS+ server.

**Options** *seconds*—Amount of time to wait.
**Range:** 1 through 90 seconds
**Default:** 3 seconds

**Usage Guidelines** See "Configuring RADIUS Authentication" on page 77 and "Configuring TACACS+ Authentication" on page 81.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** retry

## time-zone

**Syntax** time-zone (GMT<(+ | –)*hour-offset*> | *time-zone*);

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before JUNOS Release 7.4.
GMT<(+ | –)*hour-offset*> option added in JUNOS Release 7.4.

**Description** Set the local time zone. To have the time zone change take effect for all processes running on the router, you must reboot the router.

**Default** UTC

**Options** GMT<(+ | –)*hour-offset*>—Set the time zone relative to UTC time.
**Range:** –14 through +12
**Default:** NULL

*time-zone*—Specify the time zone as UTC, which is the default time zone, or as a string such as PDT (Pacific Daylight Time), or use one of the following continents and major cities:

Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek

America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Aruba, America/Asuncion, America/Barbados, America/Belize, America/Bogota, America/Boise, America/Buenos_Aires, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Cordoba, America/Costa_Rica, America/Cuiaba, America/Curacao, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/El_Salvador, America/Ensenada, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Vevay, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Maceio, America/Managua, America/Manaus, America/Martinique, America/Mazatlan, America/Mendoza, America/Menominee, America/Mexico_City, America/Miquelon, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/Panama, America/Pangnirtung, America/Paramaribo,

America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Acre, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet, America/Regina, America/Rosario, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Tortola, America/Vancouver, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife

Antarctica/Casey, Antarctica/DumontDUrville, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/South_Pole

Arctic/Longyearbyen

Asia/Aden, Asia/Alma-Ata, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hong_Kong, Asia/Irkutsk, Asia/Ishigaki, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Katmandu, Asia/Krasnoyarsk, Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Magadan, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novosibirsk, Asia/Omsk, Asia/Phnom_Penh, Asia/Pyongyang, Asia/Qatar, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Thimbu, Asia/Tokyo, Asia/Ujung_Pandang, Asia/Ulan_Bator, Asia/Urumqi, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan

Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley

Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Darwin, Australia/Hobart, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/Perth, Australia/Sydney

Europe/Amsterdam, Europe/Andorra, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Helsinki, Europe/Istanbul, Europe/Kaliningrad, Europe/Kiev, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Oslo, Europe/Paris, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Warsaw, Europe/Zagreb, Europe/Zurich

Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion

Pacific/Apia, Pacific/Auckland, Pacific/Chatham, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap

**Usage Guidelines** See “Setting the Time Zone” on page 99.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## traceoptions

See the following sections:

## *traceoptions (Address-Assignment Pool)*

**Syntax**

```
traceoptions {
    file filename{
        files number;
        size maximum-file-size;
        match regex;
        world-readable | no-world-readable
    }
    flag address-assignment;
    flag all;
    flag configuration;
    flag framework;
    flag ldap;
    flag local-authentication;
    flag radius;
}
```

**Hierarchy Level** [edit system processes general-authentication-service]

**Release Information** Flag for tracing address-assignment pool operations introduced in JUNOS Release 9.0.
option-name option introduced in JUNOS Release 8.3.

**Description** Configure tracing options.

**Options** file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.

files *number*—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.
**Range:** 2 through 1000
**Default:** 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- address-assignment—All address-assignment events
- all—All tracing operations
- configuration—Configuration events
- framework—Authentication framework events
- ldap—LDAP authentication events
- local-authentication—Local authentication events
- radius—RADIUS authentication events

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.
**Syntax:** xk to specify KB, xm to specify MB, or xg to specify GB
**Range:** 10 KB through 1 GB
**Default:** 128 KB

world-readable—(Optional) Enable unrestricted file access.

**Usage Guidelines** See "Tracing Address-Assignment Pool Processes" on page 462.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## *traceoptions (Commit Scripts)*

**Syntax**
```
traceoptions {
    file filename <files number> <size size>;
    flag flag;
}
```

**Hierarchy Level** [edit system scripts commit]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Define tracing operations for the commit scripts.

**Default** If you do not include this statement, no commit-script-specific tracing operations are performed.

**Options** *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, commit script process tracing output is placed in the file cscript.log.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option.
**Range:** 2 through 1000
**Default:** 10 files

*flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- all—Log all operations
- events—Log important events
- input—Log commit script input data
- offline—Generate data for offline development
- output—Log commit script output data
- rpc—Log commit script RPCs
- xslt—Log the XSLT library

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches its maximum size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option.

**Syntax:** *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
**Range:** 128 KB through 1 GB
**Default:** 128 KB

**Usage Guidelines** See the *JUNOS Configuration and Diagnostic Automation Guide*.

**Required Privilege Level** maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

## *traceoptions (DHCP Server on J-series Services Routers)*

**Syntax**

```
traceoptions {
   file filename <files number> <match regex> <size size> <world-readable |
      no-world-readable>;
   flag flag;
}
```

**Hierarchy Level** [edit system services dhcp]

**Release Information** Statement for tracing J-series Services Router DHCP processes introduced in JUNOS Release 8.0.

**Description** Define tracing operations for DHCP processes.

**Options** file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.
**Range:** 2 through 1000
**Default:** 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.

- all—All tracing operations
- binding—Trace binding operations
- config—Log reading of configuration
- conflict—Trace user-detected conflicts for IP addresses
- event—Trace important events
- ifdb—Trace interface database operations
- io—Trace I/O operations
- lease—Trace lease operations
- main—Trace main loop operations
- misc—Trace miscellaneous operations
- packet—Trace DHCP packets
- options—Trace DHCP options
- pool—Trace address pool operations
- protocol—Trace protocol operations
- rtsock—Trace routing socket operations

- scope—Trace scope operations
- signal—Trace DHCP signal operations
- trace—All tracing operations
- ui—Trace user interface operations

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

- all—All tracing operations
- binding—Trace binding operations
- config—Log reading of configuration
- conflict—Trace user-detected conflicts for IP addresses
- event—Trace important events
- ifdb—Trace interface database operations
- io—Trace I/O operations
- lease—Trace lease operations
- main—Trace main loop operations
- misc—Trace miscellaneous operations
- packet—Trace DHCP packets
- options—Trace DHCP options
- pool—Trace address pool operations
- protocol—Trace protocol operations
- rtsock—Trace routing socket operations
- scope—Trace scope operations
- signal—Trace DHCP signal operations
- trace—All tracing operations
- ui—Trace user interface operations
- match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches its maximum size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.
**Syntax:** *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
**Range:** 10 KB through 1 GB
**Default:** 128 KB

world-readable—(Optional) Enable unrestricted file access.

**Usage Guidelines** See "Tracing DHCP Processes" on page 162.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *traceoptions (Extended DHCP Local Server)*

**Syntax**

```
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
        regex>;
    flag flag;
}
```

**Hierarchy Level**

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
[edit logical-systems *logical-system-name* system services dhcp-local-server],
[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

**Release Information**

Statement introduced in JUNOS Release 9.0.

**Description**

Define tracing operations for DHCP processes.

**Options**

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.

files *number*—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.
**Range:** 2 through 1000
**Default:** 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- all—Trace all operations.
- auth—Trace authentication operations.
- database—Trace database events.
- fwd—Trace firewall process events.
- general—Trace miscellaneous events.
- ha—Trace high availability-related events.
- interface—Trace interface operations.
- io—Trace I/O operations.
- packet—Trace packet decoding operations.
- packet-option—Trace DHCP option decoding operations.
- rpd—Trace routing protocol process events.
- rtsock—Trace routing socket operations.
- session-db—Trace session database operations.

- state—Trace changes in state.
- ui—Trace user interface operations.

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.
**Syntax:** xk to specify KB, xm to specify MB, or xg to specify GB
**Range:** 10 KB through 1 GB
**Default:** 128 KB

world-readable—(Optional) Enable unrestricted file access.

**Usage Guidelines** See "Tracing Extended DHCP Local Server Operations" on page 175

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## tracing

**Syntax**

```
tracing {
    destination-override syslog host ip-address;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in JUNOS Release 9.2.

**Description** Configure the router to enable remote tracing to a specified host's IP address. The default setting is disabled.

The following processes are supported:

- chassisd—chassis-control process
- eventd—event-processing process
- cosd—class-of-service process
- spd—adaptive-services process

You can use the no-remote-trace statement, under the [edit system <process-name> traceoptions] hierarchy, to disable remote tracing.

**Options** destination-override syslog host *ip-address*—Overrides the global config under system tracing and has no effect if system tracing is not configured.

**Usage Guidelines** See "Tracing and Logging Operations" on page 38.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** no-remote-trace, destination-override

## transfer-interval

See the following sections:

- transfer-interval (Configuration) on page 388
- transfer-interval (System Log) on page 388

### *transfer-interval (Configuration)*

**Syntax** transfer-interval *interval*;

**Hierarchy Level** [edit system archival configuration]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the router to periodically transfer its currently active configuration to an archive site.

**Options** *interval*—Interval at which to transfer the current configuration to an archive site.
**Range:** 15 through 2880 minutes

**Usage Guidelines** See "Configuring the Transfer Interval" on page 192.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** configuration, transfer-on-commit, archive

### *transfer-interval (System Log)*

**Syntax** transfer-interval *interval*;

**Hierarchy Level** [edit system syslog file *filename* archive]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** Configure the router to periodically transfer a system log to an archive site.

**Options** *interval*—Interval at which to transfer the current configuration to an archive site.
**Range:** 5 through 2880 minutes

**Usage Guidelines** See "Specifying Log File Size, Number, and Archiving Properties" on page 123.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** archive

## transfer-on-commit

**Syntax** transfer-on-commit;

**Hierarchy Level** [edit system archival configuration]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the router to transfer its currently active configuration to an archive site each time you commit a candidate configuration.

**NOTE:** When specifying a URL in a JUNOS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example,
"ftp://*username*<:*password*>@[*ipv6-host-address*]<:*port*>/*url-path*"

**Usage Guidelines** See "Configuring Transfer on a Commit Operation" on page 193.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** configuration, transfer-interval, archive

## trusted-key

**Syntax** trusted-key [ *key-numbers* ];

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For NTP, configure the keys you are allowed to use when you configure the local router to synchronize its time with other systems on the network.

**Options** *key-numbers*—One or more key numbers. Each key can be any 32-bit unsigned integer except 0.

**Usage Guidelines** See "Configuring NTP Authentication Keys" on page 105.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** authentication-key, broadcast, peer, server

## uid

**Syntax** uid *uid-value*;

**Hierarchy Level** [edit system login user]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a user identifier for a login account.

**Options** *uid-value*—Number associated with the login account. This value must be unique on the router.
**Range:** 100 through 64000

**Usage Guidelines** See "Configuring User Access" on page 61.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## user

See the following sections:

- user (Access) on page 391
- user (System Logging) on page 392

### *user (Access)*

**Syntax**

```
user username {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication {
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
```

**Hierarchy Level** [edit system login]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure access permission for individual users.

**Options** The remaining statements are explained separately.

**Usage Guidelines** See "Configuring User Access" on page 61.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** class

## *user (System Logging)*

**Syntax**

```
user (username | *) {
    facility severity;
    match "regular-expression";
}
```

**Hierarchy Level** [edit system syslog]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the logging of system messages to user terminals.

**Options**

* (the asterisk)—Log messages to the terminal sessions of all users who are currently logged in.

*facility*—Class of messages to log. To specify multiple classes, include multiple *facility severity* statements. For a list of the facilities, see Table 19 on page 115.

*severity*—Severity of the messages that belong to the facility specified by the paired *facility* name. Messages with severities the specified level and higher are logged. For a list of the severities, see Table 20 on page 116.

*username*—JUNOS login name of the user whose terminal session is to receive system log messages. To log messages to more than one user's terminal session, include more than one user statement.

The remaining statement is explained separately.

**Usage Guidelines** See "Directing Messages to a User Terminal" on page 118.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS System Log Messages Reference*

## username-include

**Syntax**

```
username-include {
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    routing-instance-name;
    user-prefix user-prefix-string;
}
```

**Hierarchy Level**

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server group *group-name* authentication]

**Release Information**

Statement introduced in JUNOS Release 9.1.

**Description**

Configure the username that the router passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router accesses the local authentication service only and does not use external authentication services, such as RADIUS.

The statements are explained separately.

**Usage Guidelines**

See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level**

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## user-prefix

**Syntax** user-prefix *user-prefix-string*;

**Hierarchy Level**
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
[edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group *group-name* authentication username-include]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify the user prefix that is concatenated with the username during the subscriber authentication process.

**Options** *user-prefix-string*—The user prefix string.

**Usage Guidelines** See “Using External AAA Authentication Services” on page 170.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## web-management

**Syntax**

```
web-management {
    http {
        interfaces [ interface-names ];
        port port;
    }
    https {
        interfaces [ interface-names ];
        local-certificate name;
        port port;
    }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure settings for HTTP or HTTPS access. HTTP access allows management of the router using the browser-based J-Web graphical user interface. HTTPS access allows secure management of the router using the J-Web interface. With HTTPS access, communication between the router Web server and your browser is encrypted.

**Options** The remaining statements are explained separately in this chapter.

**Usage Guidelines** See the *J-Web Interface User Guide*.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** http, https, port (HTTP/HTTPS)

## wins-server

**Syntax**
```
wins-server {
    address;
}
```

**Hierarchy Level** [edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For J-series Services Routers only. Specify one or more NetBIOS Name Servers. When a DHCP client is added to the network and assigned an IP address, the NetBIOS Name Server manages the Windows Internet Name Service (WINS) database that matches IP addresses (such as 192.168.1.3) to Windows NetBIOS names (such as \\Marketing). List servers in order of preference.

**Options** *address*—IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple *address* options.

**Usage Guidelines** See "Configuring a DHCP Server" on page 147.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## world-readable

**Syntax** world-readable | no-world-readable;

**Hierarchy Level** [edit system syslog archive],
[edit system syslog file *filename* archive]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Grant all users permission to read log files, or restrict the permission only to the root user and users who have the JUNOS maintenance permission.

**Default** no-world-readable

**Usage Guidelines** See "Specifying Log File Size, Number, and Archiving Properties" on page 123.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS System Log Messages Reference*

## xnm-clear-text

**Syntax**
```
xnm-clear-text {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Allow JUNOScript clear-text requests from remote systems to the local router.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring clear-text or SSL Service for JUNOScript Client Applications" on page 146.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## xnm-ssl

**Syntax**
```
xnm-ssl {
    <connection-limit limit>;
    <rate-limit limit>;
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Allow JUNOScript SSL requests from remote systems to the local router.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring SSL Service for JUNOScript Client Applications" on page 146.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

# Part 3
# Access

Chapter 13

# Configuring Access

To configure access, include the following statements at the [edit access] hierarchy level:

```
[edit access]
address-assignment {
    pool pool-name family inet {
        network address-or-prefix </subnet-mask>;
        range name {
            low lower-limit high upper-limit;
        }
        host hostname {
            hardware-address mac-address;
            ip-address ip-address;
        }
        dhcp-attributes {
            [protocol-specific-attributes];
        }
    }
}
address-pool pool-name {
    address address-or-prefix;
    address-range low <lower-limit> high <upper-limit>;
}
group-profile profile-name {
    l2tp {
        interface-id interface-id;
        lcp-renegotiation;
        local-chap;
        maximum-sessions-per-tunnel number;
        multilink {
            drop-timeout milliseconds;
            fragmentation-threshold bytes;
        }
    }
    ppp {
        cell-overhead;
        encapsulation-overhead bytes;
        framed-pool pool-id;
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
```

```
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
    }
}
profile profile-name {
    accounting {
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        order [ accounting-method ];
        statistics (time);
        update-interval minutes;
    }
    accounting-order radius;
    authentication {
        order [ authentication-methods ];
    }
    authentication-order [ authentication-methods ];
    client client-name {
        chap-secret chap-secret;
        group-profile profile-name;
        ike {
            allowed-proxy-pair {
                remote remote-proxy-address local local-proxy-address;
            }
            pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
            ike-policy policy-name
            interface-id interface-id;
        }
        l2tp {
            interface-id interface-id;
            lcp-renegotiation;
            local-chap;
            maximum-sessions-per-tunnel number;
            multilink {
                drop-timeout milliseconds;
                fragmentation-threshold bytes;
            }
            ppp-authentication (chap | pap);
            ppp-profile profile-name;
            shared-secret shared-secret;
        }
        pap-password pap-password;
        ppp {
            cell-overhead;
            encapsulation-overhead bytes;
            framed-ip-address ip-address;
            framed-pool framed-pool;
            idle-timeout seconds;
            interface-id interface-id;
            keepalive seconds;
            primary-dns primary-dns;
            primary-wins primary-wins;
            secondary-dns secondary-dns;
            secondary-wins secondary-wins;
        }
        user-group-profile profile-name;
```

```
}
radius {
   authentication-server [ ip-address ];
   accounting-server [ ip-address ];
   options {
      accounting-session-id-format (decimal | description);
      ethernet-port-type-virtual;
      interface-description-format [ sub-interface | adapter ];
      nas-identifier identifier-value;
      nas-port-extended-format {
         adapter-width width;
         port-width width;
         slot-width width;
         stacked-vlan-width width;
         vlan-width width;
      }
      override-nas-information;
      revert-interval interval;
      vlan-nas-port-stacked-format;
   }
   attributes {
      ignore {
         framed-ip-netmask;
         input-filter;
         logical-system-routing-instance;
         output-filter;
      }
      exclude
         accounting-authentic [ accounting-on | accounting-off ];
         accounting-delay-time [ accounting-on | accounting-off ];
         accounting-session-id [ access-request | accounting-on | accounting-off |
            accounting-stop ];
         accounting-terminate-cause [ accounting-off ];
         called-station-id [ access-request | accounting-start | accounting-stop ];
         calling-station-id [ access-request | accounting-start | accounting-stop ];
         class [ accounting-start | accounting-stop ];
         dhcp-options [ access-request | accounting-start | accounting-stop ];
         dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
         dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
         output-filter [ accounting-start | accounting-stop ];
         event-timestamp [ accounting-on | accounting-off | accounting-start |
            accounting-stop ];
         framed-ip-address [ accounting-start | accounting-stop ];
         framed-ip-netmask [ accounting-start | accounting-stop ];
         input-filter [ accounting-start | accounting-stop ];
         input-gigapackets [ accounting-stop ];
         input-gigawords [ accounting-stop ];
         interface-description [ access-request | accounting-start | accounting-stop ];
         nas-identifier [ access-request | accounting-on | accounting-off |
            accounting-start | accounting-stop ];
         nas-port [ access-request | accounting-start | accounting-stop ];
         nas-port-id [ access-request | accounting-start | accounting-stop ];
         nas-port-type [ access-request | accounting-start | accounting-stop ];
         output-gigapackets [ accounting-stop ];
         output-gigawords [ accounting-stop ];
      }
```

```
        }
    }
    radius-server server-address {
        accounting-port port-number;
        port port-number;
        retry attempts ;
        routing-instance routing-instance-name;
        secret password;
        source-address source-address;
        timeout seconds;
    }
}
radius-disconnect {
    client-address {
        secret password;
    }
}
radius-disconnect-port port-number;
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
}
traceoptions {
    flag all;
    flag authentication;
    flag chap;
    flag configuration;
    flag kernel;
    flag radius;
}
```

This chapter discusses the following topics:

## Configuring the Point-to-Point Protocol

To configure the Point-to-Point Protocol (PPP), you can configure the Challenge Handshake Authentication Protocol (CHAP). CHAP allows each end of a PPP link to authenticate its peer, as defined in RFC 1994. The authenticator sends its peer a randomly generated challenge that the peer must encrypt using a one-way hash; the peer must then respond with that encrypted result. The key to the hash is a secret known only to the authenticator and authenticated. When the response is received, the authenticator compares its calculated result with the peer's response. If they match, the peer is authenticated.

Each end of the link identifies itself to its peer by including its name in the CHAP challenge and response packets it sends to the peer. This name defaults to the local hostname, or you can explicitly set it using the local-name option. When a host receives a CHAP challenge or CHAP response packet on a particular interface, it uses the peer identity to look up the CHAP secret key to use. For more information about the local-name option, see the *JUNOS Network Interfaces Configuration Guide*.

To configure CHAP, include the profile statement at the [edit access] hierarchy level:

```
[edit access]
profile profile-name {
    client client-name chap-secret chap-secret;
}
```

Then reference the CHAP profile name at the [edit interfaces] hierarchy level. For more information about how to reference CHAP, see the *JUNOS Network Interfaces Configuration Guide*.

You can configure multiple CHAP profiles, and configure multiple clients for each profile.

profile is the mapping between peer identifiers and CHAP secret keys. The identity of the peer contained in the CHAP challenge or response queries the profile for the secret key to use.

client is the peer identity.

chap-secret is the secret key associated with that peer.

The following examples show authentication using CHAP:


- Example: PPP Challenge Handshake Authentication Protocol on page 405
- Example: CHAP Authentication with RADIUS on page 406
- Configuring the Authentication Order on page 408


### *Example: PPP Challenge Handshake Authentication Protocol*

Configure the profile pe-A-ppp-clients at the [edit access] hierarchy level; then reference it at the [edit interfaces] hierarchy level:

```
[edit]
access {
```

```
    profile pe-A-ppp-clients {
      client cpe-1 chap-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcCZ0";
      # SECRET-DATA
      client cpe-2 chap-secret "$1$kdAsfaDAfkdjDsASxfafdKdFKJ";
      # SECRET-DATA
    }
  }
  interfaces {
    so-1/1/1 {
      encapsulation ppp;
      ppp-options {
        chap {
          access-profile pe-A-ppp-clients;
          local-name "pe-A-so-1/1/1";
        }
      }
    }
    so-1/1/2 {
      encapsulation ppp;
      ppp-options {
        chap {
          passive;
          access-profile pe-A-ppp-clients;
          local-name "pe-A-so-1/1/2";
        }
      }
    }
  }
```

### *Example: CHAP Authentication with RADIUS*

You can send RADIUS messages through a routing instance to customer RADIUS servers in a private network. To configure, include the routing-instance statement at the [edit access profile profile-name radius-server] hierarchy level and apply the profile to an interface with the access-profile statement at the [edit interfaces *interface-name* unit *logical-unit-number* ppp-options chap] hierarchy level.

In this example, PPP peers of interfaces at-0/0/0.0 and at-0/0/0.1 are authenticated by a RADIUS server reachable via routing instance A. PPP peers of interfaces at-0/0/0.2 and at-0/0/0.3 are authenticated by a RADIUS server reachable via routing instance B.

For more information on RADIUS authentication, see “Configuring RADIUS Authentication” on page 77.

```
system {
  radius-server {
    1.1.1.1 secret $9$dalkfj;
    2.2.2.2 secret $9$adsfaszx;
  }
}
routing-instances {
  A {
    instance-type vrf;
    ...
```

```
    }
    B {
        instance-type vrf;
        ...
    }
}
access {
    profile A-PPP-clients {
        authentication-order radius;
        radius-server {
            3.3.3.3 {
                port 3333;
                secret "$9$LO/7NbDjqmPQGDmT"; # # SECRET-DATA
                timeout 3;
                retry 3;
                source-address 99.99.99.99;
                routing-instance A;
            }
            4.4.4.4 {
                routing-instance A;
                secret $9$adsfaszx;
            }
        }
    }
    profile B-PPP-clients {
        authentication-order radius;
        radius-server {
            5.5.5.5 {
                routing-instance B;
                secret $9$kljhlkhl;
            }
            6.6.6.6 {
                routing-instance B;
                secret $9$kljhlkhl;
            }
        }
    }
}
interfaces {
    at-0/0/0 {
        atm-options {
            vpi 0;
        }
        unit 0 {
            encapsulation atm-ppp-llc;
            ppp-options {
                chap {
                    access-profile A-PPP-clients;
                }
            }
            keepalives {
                interval 20;
                up-count 5;
                down-count 5;
            }
            vci 0.128;
```

```
            family inet {
               address 21.21.21.21/32 {
                  destination 21.21.21.22;
               }
            }
         }
         unit 1 {
            encapsulation atm-ppp-llc;
            ...
            ppp-options {
               chap {
                  access-profile A-PPP-clients;
               }
            }
            ...
         }
         unit 2 {
            encapsulation atm-ppp-llc;
            ...
            ppp-options {
               chap {
                  access-profile B-PPP-clients;
               }
            }
            ...
         }
         unit 3 {
            encapsulation atm-ppp-llc;
            ...
            ppp-options {
               chap {
                  access-profile B-PPP-clients;
               }
            }
            ...
         }
         ...
      }
      ...
   }
```

Users who log in to the router with telnet or SSH connections are authenticated by the RADIUS server 1.1.1.1. The backup RADIUS server for these users is 2.2.2.2.

Each profile may contain one or more backup RADIUS servers. In this example, PPP peers are CHAP authenticated by the RADIUS server 3.3.3.3 (with 4.4.4.4. as the backup server) or RADIUS server 5.5.5.5 (with 6.6.6.6 as the backup server).

### *Configuring the Authentication Order*

You can configure the order in which the JUNOS software tries different authentication methods when authenticating peers. For each access attempt, the software tries the authentication methods in order, from first to last.

To configure the authentication order, include the authentication-order statement at the [edit access profile *name*] hierarchy level:

```
[edit access profile profile-name]
authentication-order [ authentication-methods ];
```

In *authentication-methods*, specify one or more of the following in the preferred order, from first tried to last tried:

- radius—Verify the client using RADIUS authentication services.
- password—Verify the client using the information configured at the [edit access profile *profile-name* client *client-name*] hierarchy level.

If you do not include the authentication-order statement, clients are verified by means of password authentication.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers so that the router attempts to contact each server three times, and with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 27 seconds. If you add more RADIUS servers to this configuration, they might not be contacted because the authentication process might be abandoned before these servers are tried.

The JUNOS software enforces a limit to the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—may fail to authenticate a client when this limit is exceeded. In the above example, any authentication method following this method is tried. If it fails, the authentication sequence is reinitiated by the router until authentication succeeds and the link is brought up.

## Tracing Access Processes

To trace access processes, you can specify options in the traceoptions statement at the [edit access] hierarchy level. The default tracing behavior is the following:

- Important events are logged in a file called accessd located in the /var/log directory.
- When the file accessd reaches 128 kilobytes (KB), it is renamed accessd.0, then accessd.1 and so on, until there are 3 trace files. Then the oldest trace file (accessd2. is overwritten. For more information about how log files are created, see the *JUNOS System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory (/var/log) in which trace files are located. However, you can customize the other trace file settings by including the following statements at the [edit access traceoptions] hierarchy level:

```
[edit access]
traceoptions {
   file filename {
      files number;
      size maximum-file-size;
      world-readable | no-world-readable;
      match regex;
   }
   flag all;
   flag authentication;
   flag chap;
   flag configuration;
   flag kernel;
   flag radius;
}
```

These options are described in the following sections:

- Configuring the Access Processes Log Filename on page 410
- Configuring the Number and Size of Access Processes Log Files on page 410
- Configuring Access to the Log File on page 411
- Configuring a Regular Expression for Lines to Be Logged on page 411
- Configuring the Trace Operations on page 411

### Configuring the Access Processes Log Filename

By default, the name of the file that records trace output is accessd. You can specify a different name by including the file statement at the [edit traceoptions] hierarchy level:

```
[edit access traceoptions]
file filename;
```

### Configuring the Number and Size of Access Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed *filename*.0, then *filename*.1, and so on, until there are 3 trace files. Then the oldest trace file (*filename*.2) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the [edit access traceoptions] hierarchy level:

```
[edit access traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (*filename*) reaches 2 MB, *filename* is renamed *filename*.0, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename*.0 is renamed *filename*.1 and *filename* is renamed *filename*.0. This process repeats until there are 20 trace files. Then the oldest file (*filename*.19) is overwritten by the newest file (*filename*.0).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

### Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the file world-readable statement at the [edit access traceoptions] hierarchy level:

```
[edit access traceoptions]
file world-readable;
```

To explicitly set the default behavior, include the file no-world-readable statement at the [edit event-options traceoptions] hierarchy level:

```
[edit access traceoptions]
file no-world-readable;
```

### Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the [edit access traceoptions file *filename*] hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit access traceoptions]
file filename match regex;
```

### Configuring the Trace Operations

By default, only important events are logged. You can configure the trace operations to be logged by including the following statements at the [edit access traceoptions] hierarchy level:

```
[edit access traceoptions]
flag {
   all;
   authentication;
   chap;
   configuration;
   kernel
   radius;
}
```

You can specify the following access tracing flags:

- all—All tracing operations
- authentication—All authentication module handling
- chap—All CHAP messages and handling

- configuration—Reading of configuration
- kernel—Send all configuration messages to the kernel
- radius—All RADIUS messages and handling

## Configuring the Layer 2 Tunneling Protocol

For M7i and M10i routers, you can configure Layer 2 Tunneling Protocol (L2TP) tunneling security services on an Adaptive Services Physical Interface Card (PIC) or a MultiServices PIC. The L2TP protocol allows PPP to be tunneled within a network.

**NOTE:** For information about how to configure L2TP service, see the *JUNOS Services Interfaces Configuration Guide* and the *JUNOS Network Interfaces Configuration Guide*.

To configure L2TP, include the following statements at the [edit access] hierarchy level:

```
[edit access]
address-pool pool-name {
   address address-or-prefix;
   address-range low <lower-limit> high <upper-limit>;
}
group-profile profile-name {
   l2tp {
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      ppp {
         cell-overhead;
         encapsulation-overhead bytes;
         framed-pool pool-id;
         idle-timeout seconds;
         interface-id interface-id;
         keepalive seconds;
         primary-dns primary-dns;
         primary-wins primary-wins;
         secondary-dns secondary-dns;
         secondary-wins secondary-wins;
      }
   }
   profile profile-name {
      authentication-order [ authentication-methods ];
      accounting-order radius;
      client client-name {
         chap-secret chap-secret;
         group-profile profile-name;
         l2tp {
            interface-id interface-id;
            lcp-renegotiation;
            local-chap;
```

```
            maximum-sessions-per-tunnel number;
            ppp-authentication (chap | pap);
            shared-secret shared-secret;
          }
          pap-password pap-password;
          ppp {
            cell-overhead;
            encapsulation-overhead bytes;
            framed-ip-address ip-address;
            framed-pool framed-pool;
            idle-timeout seconds;
            interface-id interface-id;
            keepalive seconds;
            primary-dns primary-dns;
            primary-wins primary-wins;
            secondary-dns secondary-dns;
            secondary-wins secondary-wins;
          }
          user-group-profile profile-name;
        }
      }
      radius-disconnect-port port-number {
        radius-disconnect {
          client-address {
            secret password;
          }
        }
      }
      radius-server server-address {
        accounting-port port-number;
        port port-number;
        retry attempts;
        secret password;
        source-address source-address;
        timeout seconds;
      }
    }
```

This section includes the following topics:

### *Minimum L2TP Configuration*

To define L2TP, include at least the following statements at the [edit access] hierarchy level:

```
[edit access]
address-pool pool-name {
   address address-or-prefix;
   address-range low <lower-limit> high <upper-limit>;
}
profile profile-name {
   authentication-order [ authentication-methods ];
   client client-name {
      chap-secret chap-secret;
      l2tp {
         interface-id interface-id;
         maximum-sessions-per-tunnel number;
         ppp-authentication (chap | pap);
         shared-secret shared-secret;
      }
      pap-password pap-password;
      ppp {
         framed-ip-address ip-address;
         framed-pool framed-pool;
         interface-id interface-id;
         primary-dns primary-dns;
         primary-wins primary-wins;
         secondary-dns secondary-dns;
         secondary-wins secondary-wins;
      }
   }
}
radius-server server-address {
   accounting-port port-number;
   port port-number;
   retry attempts;
   secret password;
}
```

**NOTE:** When the L2TP network server (LNS) is configured with RADIUS authentication, the default behavior is to accept the preferred RADIUS-assigned IP address. Previously, the default behavior was to accept and install the nonzero peer IP address received in the Internet Protocol Control Protocol (IPCP) configuration request packet. For more information about RADIUS authentication for LT2P, see "Configuring RADIUS Authentication for L2TP" on page 433.

### *Configuring the Address Pool*

With an address pool, you configure an address or address range. When you define an address pool for a client, the L2TP network server (LNS) allocates IP addresses for clients from an address pool. If you do not want to use an address pool, you can specify an IP address by means of the framed-ip-address statement at the [edit access

profile *profile-name* client *client-name* ppp] hierarchy level. For information about specifying an IP address, see "Configuring the PPP Properties for a Profile" on page 428.

**NOTE:** When an address pool is modified or deleted, all the sessions using that pool are deleted.

To define an address or a range of addresses, include the address-pool statement at the [edit access] hierarchy level:

```
[edit access]
address-pool pool-name;
```

*pool-name* is the name assigned to the address pool.

To configure an address, include the address statement at the [edit access address-pool *pool-name*] hierarchy level:

```
[edit access address-pool pool-name]
address address-or-prefix;
```

*address-or-prefix* is one address or a prefix value.

When you specify an address range, it cannot exceed 65,535 IP addresses.

To configure the address range, include the address-range statement at the [edit access address-pool *pool-name*] hierarchy level:

```
[edit access address-pool pool-name]
address-range <low lower-limit> <high upper-limit>;
```

- low *lower-limit*—The lower limit of an address range.
- high *upper-limit*—The upper limit of an address range.

**NOTE:** The address pools for user access and Network Address Translation (NAT) can overlap. When you configure an address pool at the [edit access address-pool *pool-name*] hierarchy level, you can also configure an address pool at the [edit services nat pool *pool-name*] hierarchy level, For more information about how to configure an address pool for NAT, see the *JUNOS Services Interfaces Configuration Guide*.

## *Configuring the Group Profile*

Optionally, you can configure the group profile to define the PPP or L2TP attributes. Any client referencing the configured group profile inherits all the group profile attributes.

**NOTE:** The group-profile statement overrides the user-group-profile statement, which is configured at the [edit access profile *profile-name*] hierarchy level. The profile statement overrides the attributes configured at the [edit access group-profile *profile-name*] hierarchy level. For information about the user-group-profile statement, see "Applying a Configured PPP Group Profile to a Tunnel" on page 429.

To configure the group profile, include the group-profile statement at the [edit access] hierarchy level:

```
[edit access]
group-profile profile-name;
```

*profile-name* is the name assigned to the group profile.

To configure the L2TP properties for a group profile, include the following statements at the [edit access group-profile *profile-name*] hierarchy level:

```
[edit access group-profile profile-name]
l2tp {
    interface-id interface-id;
    lcp-renegotiation;
    local-chap;
    maximum-sessions-per-tunnel number;
}
```

To configure the PPP properties for a group profile, include the following statements at the [edit access group-profile *profile-name*] hierarchy level:

```
[edit access group-profile profile-name]
ppp {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-pool pool-id;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
}
```

This section describes how to configure the group profile:



### Configuring L2TP for a Group Profile

To configure the L2TP for the group profile, include the following statements at the [edit access group-profile *profile-name* l2tp] hierarchy level:

```
[edit access group-profile profile-name l2tp]
interface-id interface-id;
lcp-renegotiation;
local-chap;
maximum-sessions-per-tunnel number;
```

*interface-id* is the identifier for the interface representing an L2TP session configured at the [edit interfaces *interface-name* unit *local-unit-number* dial-options] hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

You can configure the LNS so that it renegotiates the link control protocol (LCP) with the PPP client (in the renegotiation statement). By default, the PPP client negotiates the LCP with the L2TP access concentrator (LAC). When you do this, the LNS discards the last sent and the last received LCP configuration request attribute value pairs (AVPs) from the LAC; for example, the LCP negotiated between the PPP client and the LAC.

You can configure the JUNOS software so that the LNS ignores proxy authentication AVPs from the LAC and reauthenticates the PPP client using a CHAP challenge (in the local-chap statement). When you do this, the LNS directly authenticates the PPP client. By default, the PPP client is not reauthenticated by the LNS.

*number* is the maximum number of sessions per L2TP tunnel.

### Configuring the PPP Attributes for a Group Profile

To configure the PPP attributes for a group profile, include the following statements at the [edit access group-profile *profile-name* ppp] hierarchy level:

```
[edit access group-profile profile-name ppp]
cell-overhead;
encapsulation-overhead bytes;
framed-pool pool-id;
idle-timeout seconds;
interface-id interface-id;
keepalive seconds;
primary-dns primary-dns;
primary-wins primary-wins;
secondary-dns secondary-dns;
secondary-wins secondary-wins;
```

The cell-overhead statement configures the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping on the IQ2 PIC.

*bytes* (in the encapsulation-overhead statement) configures the number of bytes used as overhead for class-of-service calculations. For more information, see the *JUNOS Class of Service Configuration Guide*.

*pool-id* (in the framed-pool statement) is the name assigned to the address pool.

*seconds* (in the idle-timeout statement) is the number of seconds a user can remain idle before the session is terminated. By default, idle timeout is set to 0. You can configure this to be a value in the range from 0 through 4,294,967,295.

*interface-id* (in the interface-id statement) is the identifier for the interface representing an L2TP session configured at the [edit interfaces *interface-name* unit *local-unit-number* dial-options] hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

*seconds* (in the keepalive statement) is the time period that must elapse before the JUNOS software checks the status of the PPP session by sending an echo request to the peer. For each session, JUNOS software sends out three keepalives at 10-second intervals and the session is close if there is no response. By default, the time to send a keepalive messages is set to 10 seconds. You configure this to be a value in the range from 0 through 32,767.

*primary-dns* (in the primary-dns statement) is an IP version 4 (IPv4) address.

*secondary-dns* (in the secondary-dns statement) is an IPv4 address.

*primary-wins* (in the primary-wins statement) is an IPv4 address.

*secondary-wins* (in the secondary-wins statement) is an IPv4 address.

### Example: Group Profile Configuration

Configure an L2TP and PPP group profile:

```
[edit access]
group-profile westcoast_users {
    ppp {
        framed-pool customer_a;
        keepalive 15;
        primary-dns 192.120.65.1;
        secondary-dns 192.120.65.2;
        primary-wins 192.120.65.3;
        secondary-wins 192.120.65.4;
        interface-id west
    }
}
group-profile eastcoast_users {
    ppp {
        framed-pool customer_b;
        keepalive 15;
        primary-dns 192.120.65.5;
        secondary-dns 192.120.65.6;
        primary-wins 192.120.65.7;
        secondary-wins 192.120.65.8;
        interface-id east;
    }
}
group-profile westcoast_tunnel {
    l2tp {
        maximum-sessions-per-tunnel 100;
    }
}
group-profile east_tunnel {
    l2tp {
```

```
        maximum-sessions-per-tunnel 125;
    }
}
```

### *Configuring the Profile*

You can configure multiple profiles. You can also configure multiple clients for each profile. To configure the profile, include the **profile** statement at the **[edit access]** hierarchy level:

```
[edit access]
profile profile-name;
```

*profile-name* is the name assigned to the profile.

---

**NOTE:** The **group-profile** statement overrides the **user-group-profile** statement, which is configured at the **[edit access profile** *profile-name***]** hierarchy level. The **profile** statement overrides the attributes configured at the **[edit access group-profile** *profile-name***]** hierarchy level. For information about the **user-group-profile** statement, see "Applying a Configured PPP Group Profile to a Tunnel" on page 429.

When you configure a profile, you can only configure L2TP or PPP parameters. You cannot configure both.

---

To configure the L2TP properties for a profile, include the following statements at the **[edit access profile** *profile-name***]** hierarchy level:

```
[edit access profile profile-name]
authentication-order [ authentication-methods ];
accounting-order radius
client client-name {
    group-profile profile-name;
    l2tp {
        interface-id interface-id;
        lcp-renegotiation;
        local-chap;
        maximum-sessions-per-tunnel number;
        ppp-authentication (chap | pap);
        shared-secret shared-secret;
    }
}
user-group-profile profile-name;
```

To configure the PPP properties for a profile, include the following statements at the **[edit access profile** *profile-name***]** hierarchy level:

```
[edit access profile profile-name]
authentication-order [ authentication-methods ];
client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    pap-password pap-password;
```

```
    ppp {
        cell-overhead;
        encapsulation-overhead bytes;
        framed-ip-address ip-address;
        framed-pool framed-pool;
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
    }
}
```

**NOTE:** When you configure PPP properties for a profile, you typically configure the chap-secret statement or pap-password statement.

To configure the profile, do the following:

- Configuring the Authentication Order on page 420
- Configuring the Accounting Order on page 421
- Configuring the Client on page 421

### Configuring the Authentication Order

You can configure the order in which the JUNOS software tries different authentication methods when authenticating peers. For each access attempt, the software tries the authentication methods in order, from first to last.

To configure the authentication order, include the authentication-order statement at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]
authentication-order [ authentication-methods ];
```

In *authentication-methods*, specify one or more of the following in the preferred order, from first tried to last tried:

- radius—Verify the client using RADIUS authentication services.
- password—Verify the client using the information configured at the [edit access profile *profile-name* client *client-name*] hierarchy level.

**NOTE:** When you configure the authentication methods for L2TP, only the first configured authentication method is used.

For L2TP, RADIUS authentication servers are configured at the [edit access radius-server] hierarchy level. For more information about configuring RADIUS authentication servers, see "Configuring RADIUS Authentication for L2TP" on page 433.

If you do not include the authentication-order statement, clients are verified by means of password authentication.

### Configuring the Accounting Order

Beginning with JUNOS release 8.0, you can configure RADIUS accounting for an L2TP profile.

With RADIUS accounting enabled, Juniper Networks routers, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. The framework for RADIUS accounting is described in RFC 2866.

To configure RADIUS accounting, include the accounting-order statement at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]
accounting-order radius;
```

When you enable RADIUS accounting for an L2TP profile, it applies to all the clients within that profile. You must enable RADIUS accounting on at least one LT2P profile for the RADIUS authentication server to send accounting stop and start messages.

**NOTE:** When you enable RADIUS accounting for an L2TP profile, you do not need to configure the accounting-port statement at the [edit access radius-server *server-address*] hierarchy level. When you enable RADIUS accounting for an L2TP profile, accounting is triggered on the default port of 1813.

For L2TP, RADIUS authentication servers are configured at the [edit access radius-server] hierarchy level. For more information about configuring RADIUS authentication servers, see "Configuring RADIUS Authentication for L2TP" on page 433.

### Configuring the Client

To configure the client, include the client statement at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]
client client-name;
```

*client-name* is the peer identity.

For L2TP, you can optionally use the wildcard (*) to define a default tunnel client to authenticate multiple LACs with the same secret and L2TP attributes. If an LAC with a specific name is not defined in the configuration, the wildcard tunnel client authenticates it.

This section includes the following topics:



### *Example: Defining the Default Tunnel Client*

Use the wildcard (*) to define a default tunnel client to authenticate multiple LACs with the same secret:

```
[edit access profile profile-name]
client * {
   l2tp {
      interface-id interface1;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel 500;
      ppp-authentication chap;
      shared-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcCZ0";
   }
}
```

For any tunnel client, you can optionally use the user group profile to define default PPP attributes for all users coming in through a tunnel. The user group profile must define PPP attributes. If the user group profile is specified, all users (PPP sessions) use the PPP attributes specified in the user group profile. The PPP attributes specified in the local or RADIUS server take precedence over those specified in the user group profile.

Optionally, you can use a wildcard client to define a user group profile. When you do this, any client entering this tunnel uses the PPP attributes (defined user group profile attributes) as its default PPP attributes.

#### *Example: Defining the User Group Profile*

Use a wildcard client to define a user group profile:

```
[edit access profile profile]
client * {
   user-group-profile user-group-profile1;
}
```

For information about how to configure the user group profile, see "Applying a Configured PPP Group Profile to a Tunnel" on page 429.

#### *Configuring the CHAP Secret*

CHAP allows each end of a PPP link to authenticate its peer, as defined in RFC 1994. The authenticator sends its peer a randomly generated challenge that the peer must encrypt using a one-way hash; the peer must then respond with that encrypted result. The key to the hash is a secret known only to the authenticator and authenticated. When the response is received, the authenticator compares its calculated result with the peer's response. If they match, the peer is authenticated.

Each end of the link identifies itself to its peer by including its name in the CHAP challenge and response packets it sends to the peer. This name defaults to the local hostname, or you can explicitly set it using the local-name option. When a host receives a CHAP challenge or CHAP response packet on a particular interface, it uses the peer identity to look up the CHAP secret key to use. For more information about the local-name option, see the *JUNOS Network Interfaces Configuration Guide*.

**NOTE:** When you configure PPP properties for an L2TP profile, you typically configure the chap-secret statement or pap-password statement.

To configure CHAP, include the profile statement and specify a profile name at the [edit access] hierarchy level:

```
[edit access]
profile profile-name {
   client client-name chap-secret data;
}
```

Then reference the CHAP profile name at the [edit interfaces *interface-name* ppp-options chap] hierarchy level. For more information about how to reference CHAP, see the *JUNOS Network Interfaces Configuration Guide*.

You can configure multiple profiles. You can also configure multiple clients for each profile.

profile is the mapping between peer identifiers and CHAP secret keys. The identity of the peer contained in the CHAP challenge or response queries the profile for the secret key to use.

client is the peer identity.

chap-secret *secret* is the secret key associated with that peer.

#### *Example: Configuring PPP CHAP*

Configure the profile westcoast_bldg1 at the [edit access] hierarchy level, then reference it at the [edit interfaces] hierarchy level:

```
[edit]
access {
   profile westcoast_bldg1 {
      client cpe-1 chap-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcCZ0";
      # SECRET-DATA
      client cpe-2 chap-secret "$1$kdAsfaDAfkdjDsASxfafdKdFKJ";
      # SECRET-DATA
   }
}
```

#### *Referencing the Group Profile*

You can reference a configured group profile from the L2TP tunnel profile.

To reference the group profile configured at the [edit access group-profile *profile-name*] hierarchy level, include the group-profile statement at the [edit access profile *profile-name* client *client-name*] hierarchy level:

```
[edit access profile profile-name client client-name]
group-profile profile-name;
```

*profile-name* references a configured group profile from a PPP user profile.

#### *Configuring L2TP Properties for a Profile*

To define L2TP properties for a profile, include one or more of the following statements at the [edit access profile *profile-name* client *client-name* l2tp] hierarchy level:

**NOTE:** When you configure the profile, you can only configure L2TP or PPP parameters. You cannot configure both.

```
[edit access profile profile-name client client-name l2tp]
interface-id interface-id;
lcp-renegotiation;
local-chap;
maximum-sessions-per-tunnel number;
multilink {
   drop-timeout milliseconds;
   fragmentation-threshold bytes;
}
ppp-authentication (chap | pap);
shared-secret shared-secret;
```

*interface-id* (in the interface-id statement) is the identifier for the interface representing an L2TP session configured at the [edit interfaces *interface-name* unit *local-unit-number* dial-options] hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

*number* (in the maximum-sessions-per-tunnel statement) is the maximum number of sessions for an L2TP tunnel.

*shared-secret* (in the shared-secret statement) is the shared secret for authenticating the peer.

You can specify PPP authentication (in the ppp-authentication statement). By default, the PPP authentication uses CHAP. You can configure this to use Password Authentication Protocol (PAP).

You can configure LNS so it renegotiates LCP with the PPP client (in the lcp-renegotiation statement). By default, the PPP client negotiates the LCP with the LAC. When you do this, the LNS discards the last sent LCP configuration request and last received LCP configuration request AVPs from the LAC; for example, the LCP negotiated between the PPP client and LAC.

You can configure the JUNOS software so that the LNS ignores proxy authentication AVPs from the LAC and reauthenticates the PPP client using a CHAP challenge (in the local-chap statement). By default, the PPP client is not reauthenticated by the LNS. When you do this, the LNS directly authenticates the PPP client.

You can configure the PPP MP for L2TP if the PPP sessions that are coming into the LNS from the LAC have multilink PPP negotiated. When you do this, you join multilink bundles based on the endpoint discriminator (in the multilink statement).

- *milliseconds* (in the drop-timeout statement) specifies the number of milliseconds for the timeout that associated with the first fragment on the reassembly queue. If the timeout expires before all the fragments have been collected, the fragments at the beginning of the reassembly queue are dropped. If the drop timeout is not specified, the JUNOS software holds on to the fragments (fragments may still be dropped if the multilink reassembly algorithm determines that another fragment belonging to the packet on a reassembly queue has been lost).

**NOTE:** The drop timeout and fragmentation threshold for a bundled multilink might belong to different tunnels. The different tunnels might have different drop timeout and fragmentation thresholds. We recommend configuring group profiles instead of profiles when you have L2TP tunnels.

- *bytes* specifies the maximum size of a packet, in bytes (in the fragmentation-threshold statement). If a packet exceeds the fragmentation threshold, the JUNOS software fragments it into two or more multilink fragments.

#### *Example: PPP MP for L2TP*

Join multilink bundles based on the endpoint discriminator:

```
[edit access]
profile tunnel-profile {
   client remote-host {
      l2tp {
         multilink {
            drop-timeout 600;
            fragmentation-threshold 100;
         }
      }
   }
}
```

***Example: L2TP Multilink PPP Support on Shared Interfaces***

On M7i and M10i routers, L2TP multilink PPP sessions are supported on both dedicated and shared interfaces. This example shows how to configure many multilink bundles on a single ASP shared interface.

```
[edit]
interfaces {
   sp-1/3/0 {
      traceoptions {
         flag all;
      }
      unit 0 {
         family inet;
      }
      unit 20 {
         dial-options {
            l2tp-interface-id test;
            shared;
         }
         family inet;
      }
   }
}
access {
   profile t {
      client cholera {
         l2tp {
            interface-id test;
            multilink;
            shared-secret "$9$n8HX6A01RhlvL1R"; # SECRET-DATA
         }
      }
   }
   profile u {
      authentication-order radius;
   }
   radius-server {
      192.168.65.63 {
         port 1812;
         secret "$9$Vyb4ZHkPQ39mf9pORIexNdbgoZUjqP5"; # SECRET-DATA
      }
   }
```

```
}
services {
   l2tp {
      tunnel-group 1 {
         tunnel-access-profile t;
         user-access-profile u;
         local-gateway {
            address 10.70.1.1;
         }
         service-interface sp-1/3/0;
      }
      traceoptions {
         flag all;
         debug-level packet-dump;
         filter {
            protocol l2tp;
            protocol ppp;
            protocol radius;
         }
      }
   }
}
```

### *Configuring the Password Authentication Protocol Password for an L2TP Profile*

When you configure PPP properties for an L2TP profile, you typically configure the chap-secret statement or pap-password statement. For information about how to configure the CHAP secret, see "Configuring the CHAP Secret" on page 423.

To configure the Password Authentication Protocol (PAP) password, include the pap-password statement at the [edit access profile *profile-name* client *client-name*] hierarchy level:

```
[edit access profile profile-name client client-name]
pap-password pap-password;
```

*pap-password* is the password for PAP.

### *Example: Configuring PAP for an L2TP Profile*

```
[edit access]
profile sunnyvale_bldg_2 {
   client green {
      pap-password "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
      ppp {
         interface-id west;
      }
      group-profile sunnyvale_users;
   }
   client red {
      chap-secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
      group-profile sunnyvale_users;
   }
   authentication-order radius;
}
```

```
profile Sunnyvale_bldg_1_tunnel {
   client test {
      l2tp {
         shared-secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
         ppp-authentication pap;
      }
   }
}
```

### *Configuring the PPP Properties for a Profile*

To define PPP properties for a profile, include one or more of the following statements at the [edit access profile *profile-name* client *client-name* ppp] hierarchy level. The properties defined in the profile take precedence over the values defined in the group profile.

```
[edit access profile profile-name client client-name ppp]
cell-overhead;
encapsulation-overhead bytes;
framed-ip-address ip-address;
framed-pool pool-id;
idle-timeout seconds;
interface-id interface-id;
keepalive seconds;
primary-dns primary-dns;
primary-wins primary-wins;
secondary-dns secondary-dns;
secondary-wins secondary-wins;
```

**NOTE:** When you configure a profile, you can only configure L2TP or PPP parameters. You cannot configure both.

The cell-overhead statement configures the session to use ATM-aware egress shaping on the IQ2 PIC.

*bytes* (in the encapsulation-overhead statement) configures the number of bytes used as overhead for class-of-service calculations. For more information, see the *JUNOS Class of Service Configuration Guide*.

*ip-address* (in the framed-ip-address statement) is the IPv4 prefix.

*pool-id* (in the framed-pool statement) is a configured address pool.

*seconds* (in the idle-timeout statement) is the number of seconds a user can remain idle before the session is terminated. By default, idle timeout is set to 0. You can configure this to be a value in the range from 0 through 4,294,967,295.

*interface-id* (in the interface-id statement) is the identifier for the interface representing an L2TP session configured at the [edit interfaces *interface-name* unit *local-unit-number* dial-options] hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

*seconds* (in the keepalive statement) is the time period that must elapse before the JUNOS software checks the status of the PPP session by sending an echo request to the peer. For each session, JUNOS software sends out three keepalives at 10-second intervals and the session is closed if there is no response. By default, the time to send a keepalive messages is set to 10 seconds. You configure this to be a value in the range from 0 through 32,767.

*primary-dns* (in the primary-dns statement) is an IPv4 address.

*secondary-dns* (in the secondary-dns statement) is an IPv4 address.

*primary-wins* (in the primary-wins statement) is an IPv4 address.

*secondary-wins* (in the secondary-wins statement) is an IPv4 address.

### *Applying a Configured PPP Group Profile to a Tunnel*

On Mi7 and M10i routers, you can optionally apply a configured PPP group profile to a tunnel. For any tunnel client, you can use the user-group-profile statement to define default PPP attributes for all users coming in through a tunnel. The user group profile must define PPP attributes. If the user group profile is specified, all users (PPP sessions) use the PPP attributes specified in the user group profile.

When a PPP client enters a tunnel, the JUNOS software first applies the PPP user group profile attributes and then any PPP attributes from the local or RADIUS server. The PPP attributes defined in the RADIUS or local server take precedence over the attributes defined in the user group profile.

To apply configured PPP attributes to a PPP client, include the user-group-profile statement at the [edit access profile *profile-name* client *client-name*] hierarchy level:

```
[edit access profile profile-name client client-name]
user-group-profile profile-name;
```

*profile-name* is a PPP group profile configured at the [edit access group-profile *profile-name*] hierarchy level. When a client enters this tunnel, it uses the user-group-profile attributes as the default attributes.

### *Example: Applying a User Group Profile on the M7i or M10i Router*

Apply a configured PPP group profile to a tunnel:

```
[edit access]
group-profile westcoast_users {
    ppp {
        idle-timeout 100;
    }
}
group-profile westcoast_default_configuration {
    ppp {
        framed-pool customer_b;
        idle-timeout 20;
        interface-id west;
        primary-dns 192.120.65.5;
```

```
        secondary-dns 192.120.65.6;
        primary-wins 192.120.65.7;
        secondary-wins 192.120.65.8;
    }
}
profile westcoast_bldg_1_tunnel {
    client test {
        l2tp {
            interface-id west;
            shared-secret "$9$r3HKvLg4ZUDkX7JGjif5p0BIRS8LN";
            # SECRET-DATA
            maximum-sessions-per-tunnel 75;
            ppp-authentication chap;
        }
        user-group-profile westcoast_default_configuration; # Apply default PPP
    }
}
profile westcoast_bldg_1 {
    client white {
        chap-secret "$9$3s2690IeK8X7VKM7VwgaJn/Ctu1hclv87Ct87";
        # SECRET-DATA
        ppp {
            idle-timeout 22;
            primary-dns 192.120.65.9;
            framed-ip-address 12.12.12.12/32;
        }
        group-profile westcoast_users; # Reference the west_users group
    }
}
```

***Example: Configuring the Profile***

Configure the profile:

```
[edit access]
profile westcoast_bldg_1 {
    client white {
        chap-secret "$9$3s2690IeK8X7VKM7VwgaJn/Ctu1hclv87Ct87";
        # SECRET-DATA
        ppp {
            idle-timeout 22;
            primary-dns 192.120.65.10;
            framed-ip-address 12.12.12.12/32;
        }
        group-profile westcoast_users;
    }
    client blue {
        chap-secret "$9$eq1KWxbwgZUHNdjqmTF3uO1Rhr-dsoJDNd";
        # SECRET-DATA
        group-profile sunnyvale_users;
    }
    authentication-order password;
}
profile westcoast_bldg_1_tunnel {
    client test {
```

```
    l2tp {
      shared-secret "$9$r3HKvLg4ZUDkX7JGjif5p0BIRS8LN";
      # SECRET-DATA
      maximum-sessions-per-tunnel 75;
      ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
  }
  client production {
    l2tp {
      shared-secret "$9$R2QErv8X-goGylVwg4jiTz36/t0BEleWFnRh
      rlXxbs2aJDHqf3nCP5";
      # SECRET-DATA
      ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
  }
}
```

### *Example: Configuring L2TP*

Configure L2TP:

```
[edit]
access {
  address-pool customer_a {
    address 1.1.1.1/32;
  }
  address-pool customer_b {
    address-range low 2.2.2.2 high 2.2.3.2;
  }
  group-profile westcoast_users {
    ppp {
      framed-pool customer_a;
      idle-timeout 15;
      primary-dns 192.120.65.1;
      secondary-dns 192.120.65.2;
      primary-wins 192.120.65.3;
      secondary-wins 192.120.65.4;
      interface-id west;
    }
  }
  group-profile eastcoast_users {
    ppp {
      framed-pool customer_b;
      idle-timeout 20;
      primary-dns 192.120.65.5;
      secondary-dns 192.120.65.6;
      primary-wins 192.120.65.7;
      secondary-wins 192.120.65.8;
      interface-id east;
    }
  }
  group-profile westcoast_tunnel {
    l2tp {
```

```
        maximum-sessions-per-tunnel 100;
    }
}
group-profile east_tunnel {
    l2tp {
        maximum-sessions-per-tunnel 125;
    }
}
profile westcoast_bldg_1 {
    client white {
        chap-secret "$9$3s2690IeK8X7VKM7VwgaJn/Ctu1hclv87Ct87";
        # SECRET-DATA
        ppp {
            idle-timeout 22;
            primary-dns 192.120.65.10;
            framed-ip-address 12.12.12.12/32;
        }
        group-profile westcoast_users;
    }
    client blue {
        chap-secret "$9$eq1KWxbwgZUHNdjqmTF3uO1Rhr-dsoJDNd";
        # SECRET-DATA
        group-profile sunnyvale_users;
    }
    authentication-order password;
}
profile west-coast_bldg_2 {
    client red {
        pap-password "$9$3s2690IeK8X7VKM8888Ctu1hclv87Ct87";
        # SECRET-DATA
        ppp {
            idle-timeout 22;
            primary-dns 192.120.65.11;
            framed-ip-address 12.12.12.12/32;
        }
        group-profile westcoast_users;
    }
}
profile westcoast_bldg_1_tunnel {
    client test {
        l2tp {
            shared-secret "$9$r3HKvLg4ZUDkX7JGjif5p0BIRS8LN";
            # SECRET-DATA
            maximum-sessions-per-tunnel 75;
            ppp-authentication chap; #The default for PPP authentication
        }
        group-profile westcoast_tunnel;
    }
    client production {
        l2tp {
            shared-secret "$9$R2QErv8X-goGylVwg4jiTz36/t0BEIeWFnRh
            rlXxbs2aJDHqf3nCP5"; # SECRET-DATA
            ppp-authentication chap;
        }
        group-profile westcoast_tunnel;
    }
```

```
    }
    profile westcoast_bldg_2_tunnel {
        client black {
            l2tp {
                shared-secret "$9$R2QErv8X-goGylVwg4jiTz36/t0BEIeWFnRh
                rlXxbs2aJDHqf3nCP5";
                # SECRET-DATA
                ppp-authentication pap;
            }
            group-profile westcoast_tunnel;
        }
    }
}
```

### *Configuring RADIUS Authentication for L2TP*

The L2TP network server (LNS) sends RADIUS authentication requests or accounting requests. Authentication requests are sent out to the authentication server port. Accounting requests are sent to the accounting port. To configure RADIUS authentication for L2TP on an M10i or M7i router, include the following statements at the [edit access] hierarchy level:

```
[edit access]
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

**NOTE:** The RADIUS servers at the [edit access] hierarchy level are not used by the network access server process (NASD).

You can specify an accounting port number on which to contact the accounting server (in the accounting-port statement). Most RADIUS servers use port number 1813 (as specified in RFC 2866, *Radius Accounting*).

**NOTE:** If you enable RADIUS accounting at the [edit access profile *profile-name* accounting-order] hierarchy level, accounting is triggered on the default port of 1813 even if you do not specify a value for the accounting-port statement.

*server-address* specifies the address of the RADIUS authentication server (in the radius-server statement).

You can specify a port number on which to contact the RADIUS authentication server (in the port statement). Most RADIUS servers use port number 1812 (as specified in RFC 2865, *Remote Authentication Dial In User Service [RADIUS]* ).

You must specify a password in the secret statement. If a password includes spaces, enclose the password in quotation marks. The secret used by the local router must match that used by the RADIUS authentication server.

Optionally, you can specify the amount of time that the local router waits to receive a response from a RADIUS server (in the timeout statement) and the number of times that the router attempts to contact a RADIUS authentication server (in the retry statement). By default, the router waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds. By default, the router retries connecting to the server three times. You can configure this to be a value in the range from 1 through 10 times.

In the source-address statement, specify a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router interfaces.

To configure multiple RADIUS servers, include multiple radius-server statements. For information about how to configure the RADIUS disconnect server for L2TP, see "Configuring the RADIUS Disconnect Server for L2TP" on page 438.

**NOTE:** When the L2TP network server (LNS) is configured with RADIUS authentication, the default behavior is to accept the preferred RADIUS-assigned IP address. Previously, the default behavior was to accept and install the nonzero peer IP address received by the Internet Protocol Control Protocol (IPCP) configuration request packet.

For more information, see the following sections:

- Configuring RADIUS Attributes for L2TP on page 434
- Example: RADIUS Authentication for L2TP on page 438

### Configuring RADIUS Attributes for L2TP

The JUNOS software supports the following types of RADIUS attributes for L2TP:

- Juniper Networks vendor-specific attributes
- Attribute-value pairs (AVPs) defined by the Internet Engineering Task Force (IETF)
- RADIUS accounting stop and start AVPs

Juniper Networks vendor-specific RADIUS attributes are described in RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*. These attributes are encapsulated with the vendor ID set to the Juniper Networks ID number 2636. Table 33 on page 434 lists the Juniper Networks vendor-specific attributes you can configure for L2TP.

**Table 33: Juniper Networks Vendor-Specific RADIUS Attributes for L2TP**

| Attribute Name | Standard Number | Value |
|---|---|---|
| Juniper-Primary-DNS | 31 | IP address |

**Table 33: Juniper Networks Vendor-Specific RADIUS Attributes for L2TP** *(continued)*

| Attribute Name | Standard Number | Value |
|---|---|---|
| Juniper-Primary-WINS | 32 | IP address |
| Juniper-Secondary-DNS | 33 | IP address |
| Juniper-Secondary-WINS | 34 | IP address |
| Juniper-Interface-ID | 35 | String |
| Juniper-IP-Pool-Name | 36 | String |
| Juniper-Keep-Alive | 37 | Integer |

Table 34 on page 435 lists the IETF RADIUS AVPs supported for LT2P.

**Table 34: Supported IETF RADIUS Attributes for L2TP**

| Attribute Name | Standard Number | Value |
|---|---|---|
| User-Name | 1 | String |
| User-Password | 2 | String |
| CHAP-Password | 3 | String |
| NAS-IP-Address | 4 | IP address |
| NAS-Port | 5 | Integer |
| Service-Type | 6 | Integer |
| Framed-Protocol | 7 | Integer |
| Framed-IP-Address | 8 | IP address |
| Framed-IP-Netmask | 9 | IP address |
| Framed-MTU | 12 | Integer |
| Framed-Route | 22 | String |
| Session-Timeout | 27 | Integer |
| Idle-Timeout | 28 | Integer |
| Called-Station-ID | 30 | String |
| Calling-Station-ID | 31 | String |
| CHAP-Challenge | 60 | String |
| NAS-Port-Type | 61 | Integer |

**Table 34: Supported IETF RADIUS Attributes for L2TP** *(continued)*

| Attribute Name | Standard Number | Value |
|---|---|---|
| Framed-Pool | 88 | Integer |

Table 35 on page 436 lists the supported RADIUS accounting start AVPs for L2TP.

**Table 35: Supported RADIUS Accounting Start Attributes for L2TP**

| Attribute Name | Standard Number | Value |
|---|---|---|
| User-Name | 1 | String |
| NAS-IP-Address | 4 | IP address |
| NAS-Port | 5 | Integer |
| Service-Type | 6 | Integer |
| Framed-Protocol | 7 | Integer |
| Framed-IP-Address | 8 | IP address |
| Called-Station-ID | 30 | String |
| Calling-Station-ID | 31 | String |
| Acct-Status-Type | 40 | Integer |
| Acct-Delay-Time | 41 | Integer |
| Acct-Session-ID | 44 | String |
| Acct-Authentic | 45 | Integer |
| NAS-Port-Type | 61 | Integer |
| Tunnel-Client-Endpoint | 66 | String |
| Tunnel-Server-Endpoint | 67 | String |
| Acct-Tunnel-Connection | 68 | String |
| Tunnel-Client-Auth-ID | 90 | String |
| Tunnel-Server-Auth-ID | 91 | String |

Table 36 on page 437 lists the supported RADIUS accounting stop AVPs for L2TP.

**Table 36: Supported RADIUS Accounting Stop Attributes for L2TP**

| Attribute Name | Standard Number | Value |
|---|---|---|
| User-Name | 1 | String |
| NAS-IP-Address | 4 | IP address |
| NAS-Port | 5 | Integer |
| Service-Type | 6 | Integer |
| Framed-Protocol | 7 | Integer |
| Framed-IP-Address | 8 | IP address |
| Called-Station-ID | 30 | String |
| Calling-Station-ID | 31 | String |
| Acct-Status-Type | 40 | Integer |
| Acct-Delay-Time | 41 | Integer |
| Acct-Input-Octets | 42 | Integer |
| Acct-Output-Octets | 43 | Integer |
| Acct-Session-ID | 44 | String |
| Acct-Authentic | 45 | Integer |
| Acct-Session-Time | 46 | Integer |
| Acct-Input-Packets | 47 | Integer |
| Acct-Output-Packets | 48 | Integer |
| Acct-Terminate-Cause | 49 | Integer |
| Acct-Multi-Session-ID | 50 | String |
| Acct-Link-Count | 51 | Integer |
| NAS-Port-Type | 61 | Integer |
| Tunnel-Client-Endpoint | 66 | String |
| Tunnel-Server-Endpoint | 67 | String |
| Acct-Tunnel-Connection | 68 | String |
| Tunnel-Client-Auth-ID | 90 | String |
| Tunnel-Server-Auth-ID | 91 | String |

### Example: RADIUS Authentication for L2TP

```
[edit access]
profile sunnyvale_bldg_2 {
   client green {
      chap-secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
      ppp {
         interface-id west;
      }
      group-profile sunnyvale_users;
   }
   client red {
      chap-secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3";
      group-profile sunnyvale_users;
   }
   authentication-order radius;
}
radius-server {
   192.168.65.213 {
      port 1812;
      accounting-port 1813;
      secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3"; # SECRET-DATA
   }
   192.168.65.223 {
      port 1812;
      accounting-port 1813;
      secret "$9$24gGiPfz6CuQFu1EyW8VwYgZUik.5z3"; # SECRET-DATA
   }
}
radius-disconnect-port 2500;
radius-disconnect {
   192.168.65.152 secret "$9$rtkI87ws4ZDkgokPT3tpEcylWL7-VY4a";
   # SECRET-DATA
   192.168.64.153 secret "$9$gB4UHf5F/A0z30Ihr8Lbs24GDHqmTFn";
   # SECRET-DATA
   192.168.64.157 secret "$9$Hk5FCA0IhruOrv87sYGDikfTFn/t0B";
   # SECRET-DATA
   192.168.64.173 secret "$9$Hk5FCA0IhruOrv87sYGDikfTFn/t0B";
   # SECRET-DATA
}
```

## *Configuring the RADIUS Disconnect Server for L2TP*

To configure the RADIUS disconnect server to listen for disconnect requests from an administrator and process them, include the following statements at the [edit access] hierarchy level:

```
[edit access]
radius-disconnect-port port-number;
radius-disconnect {
   client-address {
      secret password;
   }
}
```

*port-number* is the server port to which the RADIUS client sends disconnect requests. The L2TP network server, which accepts these disconnect requests, is the server. You can specify a port number on which to contact the RADIUS disconnect server. Most RADIUS servers use port number 1700.

**NOTE:** The JUNOS software accepts only disconnect requests from the client address configured at the [edit access radius-disconnect *client-address*] hierarchy level.

*client-address* is the host sending disconnect requests to the RADIUS server. The client address is a valid IP address configured on one of the router interfaces.

*password* authenticates the RADIUS client. Passwords can contain spaces. The secret used by the local router must match that used by the server.

For information about how to configure RADIUS authentication for L2TP, see "Configuring RADIUS Authentication for L2TP" on page 433.

#### Example: Configuring the RADIUS Disconnect Server

Configure the RADIUS disconnect server:

```
[edit access]
radius-disconnect-port 1700;
radius-disconnect {
    192.168.64.153 secret "$9$rtkI87ws4ZDkgokPT3tpEcylWL7-VY4a";
    # SECRET-DATA
    192.168.64.162 secret "$9$rtkI87ws4ZDkgokPT3tpEcylWL7-VY4a";
    # SECRET-DATA
}
```

### *Configuring RADIUS Authentication for an L2TP Profile*

On an M10i or M7i routing platform, L2TP supports RADIUS authentication and accounting for users with one set of RADIUS servers under the [edit access] hierarchy. You can also configure RADIUS authentication for each tunnel client or user profile.

To configure the RADIUS authentication for L2TP tunnel clients on an M10i or M7i routing platform, include the ppp-profile statement with the l2tp attributes for tunnel clients:

```
[edit access profile profile-name client client-name l2tp]
ppp-profile profile-name;
```

ppp-profile *profile-name* specifies the profile used to validate PPP session requests through L2TP tunnels. Clients of the referenced profile must have only PPP attributes. The referenced group profile must be defined.

To configure the RADIUS authentication for a profile, include following statements at the [edit access profile *profile-name*] hierarchy level:

```
[edit access profile profile-name]
```

```
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

When a PPP user initiates a session and RADIUS authentication is configured for the user profile on the tunnel group, the following priority sequence is used to determine which RADIUS server is used for authentication and accounting:

- If the ppp-profile statement is configured under the tunnel client (LAC), the RADIUS servers configured under the specified ppp-profile are used.
- If RADIUS servers are configured under the user profile for the tunnel group, those servers will be used.
- If no RADIUS server is configured for the tunnel client (LAC) or user profile, then the RADIUS servers configured at the [edit access] hierarchy level are used.

### Example: RADIUS Authentication for an L2TP Profile

Configure RADIUS authentication for an L2TP profile:

```
[edit access]
profile t {
    client LAC_A {
        l2tp {
            ppp-profile u;
        }
    }
}
profile u {
    client client_1 {
        ppp {
        }
    }
    5.5.5.5 {
        port 3333;
        secret $9$dkafeqwrew;
        source-address 1.1.1.1;
        retry 3;
        timeout 3;
    }
    6.6.6.6 secret $9$fe3erqwrez;
    7.7.7.7 secret $9$f34929ftby;
}
```

## Configuring an Internet Key Exchange (IKE) Access Profile

An IKE access profile is used to negotiate IKE and IPSec security associations with dynamic peers. You can configure only one tunnel profile per service set for all dynamic peers. The configured preshared key in the profile is used for IKE authentication of all dynamic peers terminating in that service set. Beginning with JUNOS Release 8.2, you can also use the digital certificate method for IKE authentication with dynamic peers. Include the ike-policy *policy-name* statement at the [edit access profile *profile-name* client * ike] hierarchy level. *policy-name* is the name of the IKE policy you define at the [edit services ipsec-vpn ike policy *policy-name*] hierarchy level. For more information, see the *JUNOS Services Interfaces Configuration Guide*.

The IKE tunnel profile specifies all the information you need to complete the IKE negotiation. Each protocol has its own statement hierarchy within the client statement to configure protocol-specific attribute value pairs, but only one client configuration is allowed for each profile. The following is the configuration hierarchy.

```
[edit access]
profile profile-name {
    client * {
        ike {
            allowed-proxy-pair {
                remote remote-proxy-address local local-proxy-address;
            }
            pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
            ike-policy policy-name;
            initiate-dead-peer-detection;
            interface-id string-value;
        }
    }
}
```

For dynamic peers, the JUNOS software supports only IKE main mode with both the preshared key and digital certificate methods. In this mode, an IPv6 or IPv4 address is used to identify a tunnel peer to obtain the preshared key or digital certificate information. The client value * (wildcard) means that configuration within this profile is valid for all dynamic peers terminating within the service set accessing this profile.

The following statement makes up the IKE profile:

- allowed-proxy-pair—During phase 2 IKE negotiation, the remote peer supplies its network address (remote) and its peer's network address (local). Since multiple dynamic tunnels are authenticated through the same mechanism, this statement must include the list of possible combinations. If the dynamic peer does not present a valid combination, the phase 2 IKE negotiation fails.

By default, remote 0.0.0.0/0 local 0.0.0.0/0 is used if no values are configured.

- pre-shared-key—Key used to authenticate the dynamic peer during IKE phase 1 negotiation. This key is known to both ends through an out-of-band secure mechanism. You can configure the value either in hexadecimal or ascii-text format. It is a mandatory value.
- ike-policy—Name of the IKE policy that defines either the local digital certificate or the pre-shared key used to authenticate the dynamic peer during IKE negotiation. You must include this statement to use the digital certificate method for IKE authentication with a dynamic peer. You define the IKE policy at the [edit services ipsec-vpn ike policy *policy-name*] hierarchy level. For more information, see the *JUNOS Services Interfaces Configuration Guide*.
- initiate-dead-peer-detection—Detects dead peers on dynamic IPSec tunnels..
- interface-id—Interface identifier, a mandatory attribute used to derive the logical service interface information for the session.

For more information about how to configure IPSec tunnels with dynamic peer security gateways, see the *JUNOS Feature Guide* and the *JUNOS Services Interfaces Configuration Guide*.

## Managing Subscriber Access

The subscriber access management feature enables you to manage the subscribers that are allowed access to the network server, the services that authorized subscribers can use, and how accounting statistics are collected. The subscriber access management feature uses the AAA Service Framework to support the configuration and management of broadband subscriber access. You can statically configure different client types, such as DHCP-based subscribers, and specify the authentication, accounting, and service for the subscribers.

### *AAA Service Framework Overview*

The AAA Service Framework provides a single point of contact for all the authentication, authorization, accounting, and address assignment services that the router supports for network access. The framework supports authentication and authorization through external servers, such as RADIUS, and the Local Authentication Server component of the framework. The framework also supports accounting through external servers, and address assignment through a combination of local address assignment pools and RADIUS.

When interacting with external back-end RADIUS servers, the AAA Service Framework supports standard RADIUS attributes and Juniper Networks vendor specific attributes

(VSAs). The AAA Service Framework also includes an integrated RADIUS client that is compatible with RADIUS servers that conform to RFC-2865, RFC-2866, and RFC-3576, and which can initiate requests.

You create the following types of configurations to manage subscriber access.

- Authentication—Authentication parameters defined in the access profile determine the authentication component of the AAA processing. For example, subscribers can be authenticated using a remote authentication service such as RADIUS. You can also use the Local Authentication Server component of the AAA framework, which authenticates subscribers based on preconfigured credentials.
- Accounting— Accounting parameters in the access profile specify the accounting part of the AAA processing. For example, the parameters determine how the router collects and uses subscriber statistics.
- Address assignment—The AAA Service Framework assigns addresses to subscribers based on the configuration of local address assignment pools. For example, the AAA framework collaborates with RADIUS servers to assign addresses from the specified pools. See “Configuring Address-Assignment Pools” on page 457.

## Using RADIUS Authentication and Accounting for Subscriber Access Management

To configure the router to use RADIUS authentication and accounting for the subscriber access management feature, you create access profiles that specify the following levels of configuration. Subscriber access management supports access profiles attached at the [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*] hierarchy level.

- Router interaction with RADIUS servers—Specify how the router interacts with RADIUS servers, such as the ports used for authentication and accounting, the number of times the router tries to contact a RADIUS server, and passwords.
- Authentication and accounting parameters—Create the access profile that defines authentication and accounting parameters, such as the authentication or accounting methods to use, and how accounting statistics are collected and used.
- RADIUS parameters—Specify the RADIUS servers and options for authentication and accounting, and define how RADIUS attributes are used.

The following sections describe RADIUS authentication and accounting configuration for the subscriber access management feature:


- Configuring How the Router Interacts with RADIUS Servers on page 444
- Configuring Authentication and Accounting Parameters on page 444
- Configuring RADIUS Parameters on page 446
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 450
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 451

- Attaching Access Profiles on page 457
- Verifying and Managing Subscriber Access Information on page 457


### Configuring How the Router Interacts with RADIUS Servers

To identify the RADIUS servers that the router can use and to configure how the router interacts with the servers, you include the radius-server statement at the [edit access] hierarchy level. You can specify multiple RADIUS servers on the network.

```
[edit access]
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

The following list describes the radius-server configuration statements:

- *server-address*—The address of the RADIUS server to use. To configure more than one RADIUS server, include multiple *server-address* entries.
- accounting-port—The RADIUS server accounting port number. The default accounting port number is 1813.
- port-number—The port number used to contact the RADIUS server. The default is port number 1812.
- retry—The number of times that the router attempts to contact a RADIUS accounting server. You can configure the router to retry from 1 through 16 times. The default setting is 3 retry attempts.
- secret—The required secret (password) that the local router passes to the RADIUS client. Secrets can contain spaces.
- source-address—A source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router interfaces.
- timeout—The length of time that the local router waits to receive a response from a RADIUS server. By default, the router waits 3 seconds. You can configure the timeout to be from 1 to 90 seconds.

### Configuring Authentication and Accounting Parameters

You use an access profile to configure authentication and accounting support for the subscriber access management feature. The access profile enables you to specify the type of methods used for authentication and accounting. You can also configure how subscriber access management collects and uses accounting statistics.

### Specifying the Authentication and Accounting Methods

To specify the authentication and accounting methods that subscriber access management uses, you include the **authentication-order** statement and **accounting order** statements at the [**edit access profile** *profile-name*] hierarchy level.

```
[edit access profile profile-name]
authentication-order [ authentication-methods ]
}
accounting {
   order [ accounting-methods ];
}
```

You can configure multiple authentication and accounting methods—the **authentication-order** and **accounting order** statements specify the order in which the subscriber access management feature uses the methods. For example, an authentication entry of **radius none** specifies that RADIUS authentication is performed first and, if it fails, no authentication (**none**) is done.

```
[edit access profile profile-name]
authentication-order radius none;
```

You can specify the following authentication methods:

- **none**—No authentication
- **password**—Local authentication
- **radius**—RADIUS-based authentication

You can specify the following accounting methods:

- **radius**—RADIUS-based accounting

### Configuring How Accounting Statistics Are Collected

Include the **accounting** statement at the [**edit access profile profile-name**] hierarchy level to specify how the subscriber access management feature collects and uses accounting statistics.

```
[edit access profile profile-name]
accounting {
   accounting-stop-on-access-deny;
   accounting-stop-on-failure;
   order [ accounting-method ];
   statistics (time);
   update-interval minutes;
}
```

The following list describes the accounting statements:

- **accounting-stop-on-access-deny**—Configures AAA to issue an Acct-Stop message if the AAA server denies access to the subscriber.
- **accounting-stop-on-failure**—Configures the AAA servers to send an Acct-Stop message if the subscriber fails AAA but is granted access by the AAA-server.

- order—The order in which multiple accounting methods are used. For example, an entry of radius specifies that the router use RADIUS accounting and, if that fails, no accounting is performed.
- statistics—The types of statistics to gather. Currently, only time statistics are gathered.
- update-interval—Configures the number of minutes between accounting updates. You can configure an interval from 10 to 1440 minutes. If you specify an interval between 10 and 15, the interval is rounded up to 15.

## *Configuring RADIUS Parameters*

Include the radius statement at the [edit access profile *profile-name*] hierarchy level to specify the RADIUS parameters for the subscriber access manager feature. You can specify the IP addresses of the RADIUS servers used for authentication and accounting, options that provide configuration information for the RADIUS servers, and how RADIUS attributes are used.

### Specifying the RADIUS Authentication and Accounting Servers to Use for Subscriber Access Management

To specify one or more RADIUS authentication or accounting servers to use for subscriber access management, include the authentication-server and accounting-server statements at the [edit access profile profile-name radius] hierarchy level. You must specify the IP address for the authentication or accounting server.

```
[edit access profile profile-name radius]
authentication-server [ ip-address ];
accounting-server [ ip-address ];
```

To configure multiple RADIUS authentication or accounting servers, include multiple *ip-address* entries, for example:

```
[edit access profile profile-name radius]
authentication-server 192.168.1.1 192.168.1.2 192.168.1.3;
accounting-server 192.168.1.1 192.168.1.3 192.168.1.4;
```

### Configuring Options for RADIUS Servers

Include the options statement at the [edit access profile *profile-name* radius] hierarchy level to specify the options used by the RADIUS authentication and accounting servers.

```
[edit access profile profile-name radius]
options {
    accounting-session-id-format (decimal | description);
    ethernet-port-type-virtual;
    interface-description-format [sub-interface | adapter];
    nas-identifier identifier-value;
    nas-port-extended-format {
        adapter-width width;
        port-width width;
        slot-width width;
```

```
        stacked-vlan-width width;
        vlan-width width;
    }
    override-nas-information;
    revert-interval interval;
    vlan-nas-port-stacked-format;
}
```

The following list describes the accounting options:

- accounting-session-id-format—The format the router uses to identify the accounting session. The identifier can be in one of the following formats. The router uses decimal format by default.
  - decimal—For example, 435264
  - description—In the format, jnpr *interface-specifier*:*subscriber-session-id*. For example, jnpr fastEthernet 3/2.6:1010101010101
- ethernet-port-type-virtual—The physical port type the router uses to authenticate clients. The port type is passed in RADIUS attribute 61 (NAS-Port-Type). This statement specifies a port type of virtual; by default the router passes a port type of ethernet in RADIUS attribute 61.
- interface-description-format—The information that is included in or omitted from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the router includes both the subinterface and the adapter in the interface description.
- nas-identifier—The value for the client RADIUS attribute 32 (NAS-Identifier), which is used for authentication and accounting requests. You can specify a string in the range 1 to 64 characters.
- nas-port-extended-format—Configures the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.
  - adapter-width *width*—Number of bits in the adapter field.
  - port-width *width*—Number of bits in the port field.
  - slot-width *width*—Number of bits in the slot field.
  - stacked-vlan-width *width*—Number of bits in the SVLAN ID field.
  - vlan-width *width*—Number of bits in the VLAN ID field.
- revert-interval—The amount of time that the router waits after a server has become unreachable. The router rechecks the connection to the server when the revert-interval expires. If the server is then reachable, it is used in accordance with the order of the server list.
- vlan-nas-port-stacked-format—Configures RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

### Configuring How RADIUS Attributes Are Used

Include the attributes statement at the [edit access profile *profile-name* radius] hierarchy level to specify attributes that are ignored in RADIUS Access-Accept messages, or that are excluded from particular RADIUS message types.

```
[edit access profile profile-name radius]
attributes {
    ignore {
        framed-ip-netmask;
        input-filter;
        logical-system-routing-instance;
        output-filter;
    }
    exclude
        accounting-authentic [ accounting-on | accounting-off ];
        accounting-delay-time [ accounting-on | accounting-off ];
        accounting-session-id [ access-request | accounting-on | accounting-off |
            accounting-stop ];
        accounting-terminate-cause [ accounting-off ];
        called-station-id [ access-request | accounting-start | accounting-stop ];
        calling-station-id [ access-request | accounting-start | accounting-stop ];
        class [ accounting-start | accounting-stop ];
        dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
        dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
        output-filter [ accounting-start | accounting-stop ];
        event-timestamp [ accounting-on | accounting-off | accounting-start |
            accounting-stop ];
        framed-ip-address [ accounting-start | accounting-stop ];
        framed-ip-netmask [ accounting-start | accounting-stop ];
        input-filter [ accounting-start | accounting-stop ];
        input-gigapackets [ accounting-stop ];
        input-gigawords [ accounting-stop ];
        interface-description [ access-request | accounting-start | accounting-stop ];
        nas-identifier [ access-request | accounting-on | accounting-off | accounting-start
            | accounting-stop ];
        nas-port [ access-request | accounting-start | accounting-stop ];
        nas-port-id [ access-request | accounting-start | accounting-stop ];
        nas-port-type [ access-request | accounting-start | accounting-stop ];
        output-gigapackets [ accounting-stop ];
        output-gigawords [ accounting-stop ];
    }
}
```

The following list describes the ignore and exclude statements:

- Use the ignore statement to configure the router to ignore a particular attribute in RADIUS Access-Accept messages. By default, the router processes the attributes received from the external AAA server. You can specify that the following attributes be ignored:
  - framed-ip-netmask—Framed-Ip-Netmask, RADIUS attribute 9
  - input-filter—Ingress-Policy-Name, VSA 26-10

- logical-system-routing-instance—Virtual-Router, VSA 26-1
- output-filter—Egress-Policy-Name, VSA 26-11

- Use the exclude statement to configure the router to exclude the specified attributes from the specified type of RADIUS message. Not all attributes appear in all types of RADIUS messages—the CLI indicates the RADIUS message type. By default, the router includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages. You can configure the router to exclude the following attributes:
  - accounting-authentic—RADIUS attribute 45, Acct-Authentic
  - accounting-delay-time—RADIUS attribute 41, Acct-Delay-Time
  - accounting-session-id—RADIUS attribute 44, Acct-Session-Id
  - accounting-terminate-cause—RADIUS attribute 49, Acct-Terminate-Cause
  - called-station-id—RADIUS attribute 30, Called-Station-Id
  - calling-station-id—RADIUS attribute 31, Calling-Station-Id
  - class—RADIUS attribute 25, Class
  - dhcp-gi-address—Juniper VSA 26-57, DHCP-GI-Address
  - dhcp-mac-address—Juniper VSA 26-56, DHCP-MAC-Address
  - event-timestamp—RADIUS attribute 55, Event-Timestamp
  - framed-ip-address—RADIUS attribute 8, Framed-IP-Address
  - framed-ip-netmask—RADIUS attribute 9, Framed-IP-Netmask
  - input-filter—Juniper VSA 26-10, Ingress-Policy-Name
  - input-gigapackets—Juniper VSA 26-42, Acct-Input-Gigapackets
  - input-gigawords—RADIUS attribute 52, Acct-Input-Gigawords
  - interface-description—Juniper VSA 26-53, Interface-Desc
  - nas-identifier—RADIUS attribute 32, NAS-Identifier
  - nas-port—RADIUS attribute 5, NAS-Port
  - nas-port-id—RADIUS attribute 87, NAS-Port-Id
  - nas-port-type—RADIUS attribute 61, NAS-Port-Type
  - output-filter—Juniper VSA 26-11, Egress-Policy-Name
  - output-gigapackets—Juniper VSA 25-43, Acct-Output-Gigapackets
  - output-gigawords—RADIUS attribute 53, Acct-Output-Gigawords

### *Example: Configuring RADIUS-Based Subscriber Authentication and Accounting*

This section shows a sample RADIUS-based authentication and accounting configuration.

```
[edit access]
radius-server {
    192.168.1.250 {
        port 1812;
        accounting-port 1813;
        retry 3;
        secret &tIUEI*7688+;
        source-address 192.168.1.100;
        timeout 45;
    }
    192.168.1.251 {
        port 1812;
        accounting-port 1813;
        retry 3;
        secret $Dyu*UY(877-;
        source-address 192.168.1.100;
        timeout 30;
    }
    192.168.1.252 {
        port 1812;
        secret $Dyu*UY(877-;
    }
}
profile isp-bos-metro-fiber-basic {
    authentication {
        order radius none;
    }
    accounting {
        order radius;
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        immediate-update;
        statistics time;
        update-interval 12;
    }
    radius {
        authentication-server 192.168.1.251 192.168.1.252;
        accounting-server 192.168.1.250 192.168.1.251;
        options {
            accounting-session-id-format decimal;
            nas-identifier 56;
            override-nas-information;
        }
        attributes {
            ignore {
                framed-ip-netmask;
            }
            exclude {
                accounting-delay-time [ accounting-on | accounting-off ];
                accounting-session-id [ access-request | accounting-on | accounting-off
                | accounting-start accounting-stop ];
```

```
            dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
            dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
            nas-identifier [ access-request | accounting-start | accounting-stop ];
            nas-port [ access-request | accounting-start | accounting-stop ];
            nas-port-id [ access-request | accounting-start | accounting-stop ];
            nas-port-type [ access-request | accounting-start | accounting-stop ];
        }
    }
  }
}
[edit logical-systems isp-bos-metro-12 routing-instances isp-cmbrg-12-32]
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.168.1.100/24;
      }
    }
  }
  ge-0/0/0 {
    vlan-tagging;
    unit 0 {
      vlan-id 200;
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
}
```

## *RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework*

The AAA Service Framework supports RADIUS attributes and vendor-specific attributes (VSAs)—this support provides tunable parameters that the subscriber access management feature uses when creating subscribers and services.

RADIUS attributes are carried as part of standard RADIUS request and reply messages. The subscriber management access feature uses the RADIUS attributes to exchange specific authentication, authorization and accounting information. VSAs allow the subscriber access management feature to pass implementation-specific information that provide extended capabilities, such as service activation or deactivation, and enabling and disabling filters.

Table 37 on page 452 describes the supported RADIUS IETF attributes.
Table 38 on page 454 describes the supported Juniper Networks VSAs.

### RADIUS IETF Attributes Supported by the AAA Service Framework

Table 37 on page 452 describes the RADIUS IETF attributes supported by the JUNOS software AAA Service Framework.

**Table 37: Supported RADIUS IETF Attributes**

| Attribute Number | Attribute Name | Description |
|---|---|---|
| 1 | User-Name | ■ Name of user to be authenticated<br>■ Configurable username override |
| 2 | User-Password | ■ Password of user to be authenticated by Password Authentication Protocol (PAP)<br>■ Configurable password override |
| 4 | NAS-IP-Address | IP address of the network access server (NAS) that is requesting authentication of the user |
| 5 | NAS-Port | Physical port number of the NAS that is authenticating the user |
| 6 | Service-Type | Type of service the user has requested or the type of service to be provided |
| 8 | Framed-IP-Address | ■ IP address to be configured for the user<br>■ 0.0.0.0 or absence is interpreted as 255.255.255.254 |
| 9 | Framed-IP-Netmask | ■ IP network to be configured for the user when the user is a router to a network<br>■ Absence implies 255.255.255.255 |
| 11 | Filter-ID | ■ Name of the filter list for the user<br>■ Interpreted as input policy name |
| 12 | Framed-MTU | ■ Maximum Transmission Unit to be configured for the user when it is not negotiated by some other means (such as PPP).<br>■ When sent in an Access-Request with an EAP-Message, indicates the maximum size of the EAP-Message string that the external server supports. |
| 18 | Reply-Message | ■ Text that may be displayed to the user<br>■ Only the first instance of this attribute is used |
| 22 | Framed-Route | String that provides routing information to be configured for the user on the NAS; in the format:<br><addr>[/<maskLen>] [<nexthop> [<cost>]] (tag <tagValue>] [distance <distValue>] |
| 25 | Class | Arbitrary value that the NAS includes in all accounting packets for the user if supplied by the RADIUS server |
| 27 | Session-Timeout | Maximum number of consecutive seconds of service to be provided to the user before termination of the session |
| 32 | NAS-Identifier | NAS originating the request |

**Table 37: Supported RADIUS IETF Attributes** *(continued)*

| Attribute Number | Attribute Name | Description |
|---|---|---|
| 40 | Acct-Status-Type | Indicates whether this Accounting-Request marks the beginning of the user service (Start), the end (Stop), or the interim (Interim-Update) |
| 41 | Acct-Delay-Time | Indicates how many seconds the client has been trying to send a particular record |
| 42 | Acct-Input-Octets | Number of octets received from the port during the time this service has been provided |
| 43 | Acct-Output-Octets | Number of octets sent to the port during the time this service has been provided |
| 44 | Acct-Session-ID | Unique accounting identifier that makes it easy to match start and stop records in a log file. The identifier can be in one of the following formats:<br>■ decimal—For example, 435264<br>■ description—In the generic format, jnpr *interface-specifier*:*subscriber-session-id*; For example, jnpr fastEthernet 3/2.6:1010101010101 |
| 45 | Acct-Authentic | User authentication method: RADIUS, the NAS itself, or another remote authentication protocol |
| 46 | Acct-Session-Time | Indicates how long in seconds that the user has received service |
| 47 | Acct-Input-Packets | Number of packets received from the port during the time this service has been provided to a framed user |
| 48 | Acct-Output-Packets | Number of packets sent to the port in the course of delivering this service to a framed user |
| 49 | Acct-Terminate-Cause | Reason why the service (a PPP session) was terminated. The service can be terminated for the following reasons:<br>■ User Request (1)—User initiated the disconnect (log out)<br>■ Idle Timeout (4)—Idle timer has expired<br>■ Session Timeout (5)—Client reached the maximum continuous time allowed on the service or session<br>■ Admin Reset (6)—System administrator terminated the session<br>■ Port Error (8)—PVC failed; no hardware or no interface<br>■ NAS Error (9)—Negotiation failures, connection failures, or address lease expiration<br>■ NAS Request (10)—PPP challenge timeout, PPP request timeout, tunnel establishment failure, PPP bundle failure, IP address lease expiration, PPP keep-alive failure, tunnel disconnect, or an unaccounted-for error |

**Table 37: Supported RADIUS IETF Attributes** *(continued)*

| Attribute Number | Attribute Name | Description |
|---|---|---|
| 52 | Acct-Input-Gigawords | Number of times the Acct-Input-Octets counter has wrapped around 2^32 during the time this service has been provided. Can be present in Accounting-Request records only where the Acct-Status-Type is set to Stop or Interim-Update |
| 53 | Acct-Output-Gigawords | Number of times the Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service. Can be present in Accounting-Request records only where the Acct-Status-Type is set to Stop or Interim-Update |
| 55 | Event-Timestamp | Time that this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC |
| 61 | NAS-Port-Type | Type of physical port the NAS is using to authenticate the user |
| 85 | Acct-Interim-Interval | Number of seconds between each interim accounting update for this session |
| 87 | NAS-Port-ID | Text string that identifies the physical interface of the NAS that is authenticating the user |
| 88 | Framed-Pool | Name of an assigned address pool that should be used to assign an address for the user |

## Juniper Networks VSAs Supported by the AAA Service Framework

Table 38 on page 454 describes Juniper Networks VSAs supported by the JUNOS software AAA Service Framework. The AAA Service Framework uses vendor ID 4874, which is assigned to Juniper Networks by the Internet Assigned Numbers Authority (IANA).

**Table 38: Supported Juniper Networks VSAs**

| Attribute Number | Attribute Name | Description | Value |
|---|---|---|---|
| 26-4 | Primary-DNS | Client DNS address negotiated during IPCP | integer: 4-byte primary-dns-address |
| 26-5 | Secondary-DNS | Client DNS address negotiated during IPCP | integer: 4-byte secondary-dns-address |
| 26-6 | Primary-WINS | Client WINS (NBNS) address negotiated during IPCP | integer: 4-byte primary-wins-address |

**Table 38: Supported Juniper Networks VSAs** *(continued)*

| Attribute Number | Attribute Name | Description | Value |
|---|---|---|---|
| 26-7 | Secondary-WINS | Client WINS (NBNS) address negotiated during IPCP | integer: 4-byte secondary-wins-address |
| 26-10 | Ingress-Policy-Name | Input policy name to apply to client interface | string: input-policy-name |
| 26-11 | Egress-Policy-Name | Output policy name to apply to client interface | string: output-policy-name |
| 26-12 | Ingress-Statistics | Enable or disable input statistics on client interface | integer:<br>■ 0 = disable<br>■ 1 = enable |
| 26-13 | Egress-Statistics | Enable or disable output statistics on client interface | integer:<br>■ 0 = disable<br>■ 1 = enable |
| 26-23 | IGMP-Enable | Enable or disable IGMP on a client interface | integer:<br>■ 0 = disable<br>■ 1 = enable |
| 26-34 | Framed-IP-Route-Tag | Route tag to apply to returned framed-ip-address | integer: 4-octet |
| 26-42 | Input-Gigapackets | Number of times input-packets attribute rolls over its 4-octet field | integer |
| 26-43 | Output-Gigapackets | Number of times output-packets attribute rolls over its 4-octet field | integer |
| 26-56 | DHCP-MAC-Address | Client MAC address | string: mac-address |
| 26-57 | DHCP-GI-Address | DHCP relay agent IP address | integer: 4-octet |
| 26-63 | Interface | Text string that identifies the subscriber's access interface | string: interface-description |
| 26-65 | Activate-Service | Service to activate for the subscriber | string: service-name |

**Table 38: Supported Juniper Networks VSAs** *(continued)*

| Attribute Number | Attribute Name | Description | Value |
|---|---|---|---|
| 26-66 | Deactivate-Service | Service to deactivate for the subscriber | string: service-name |
| 26-70 | Ignore-DF-Bit | Enable or disable the ignore don't fragment (DF) bit feature on a client interface | integer:<br>■ 0 = disable<br>■ 1 = enable |
| 26-71 | IGMP-Access-Group-Name | Access List to use for the group (G) filter | string: 32-octet |
| 26-72 | IGMP-Access-Source-Group-Name | Access List to use for the source-group (S,G) filter | string: 32-octet |
| 26-74 | MLD-Access-Group-Name | Access List to use for the group (G) filter | string: 32-octet |
| 26-75 | MLD-Access-Source-Group-Name | Access List to use for the source-group (S,G) filter | string: 32-octet |
| 26-77 | MLD-Version | MLD Protocol Version | integer: 1-octet<br>■ 1 = MLD version<br>■ 2 = MLD version |
| 26-78 | IGMP-Version | IGMP Protocol Version | integer: 1-octet<br>■ 1 = IGMP version<br>■ 2 = IGMP version<br>■ 3 = IGMP version |
| 26-83 | Acct-Service-Session | Name of the service (including parameter values) that is associated with service manager statistics | string: service-name |
| 26-97 | IGMP-Immediate-Leave | IGMP Immediate Leave | integer: 4-octet<br>■ 0 = disable<br>■ 1 = enable |
| 26-100 | MLD-Immediate-Leave | MLD Immediate Leave | integer: 4-octet<br>■ 0 = disable<br>■ 1 = enable |

### *Attaching Access Profiles*

Once you have created the access profile that specifies the subscriber access management authentication and accounting parameters, you attach the profile. Subscriber access management supports access profiles attached at the [edit logical-systems *logical-instance-name* routing-instances *routing-instance-name*] level of this hierarchy.

```
[edit logical-systems logical-system-name routing-instances routing-instance-name]
access-profile profile-name;
```

For example:

```
[edit logical-systems isp22-bos-metro-12 routing-instances isp22-cmbrg-12-32]
access-profile vz-bos-metro-fios-basic;
```

### *Verifying and Managing Subscriber Access Information*

To display subscriber access statistics and information, use the following operational commands:

- show network-access aaa statistics
- show network-access aaa subscribers

To clear subscriber access statistics and to log out specific subscribers, use the following operational command:

- clear network-access aaa subscribers

For information about using these operational commands, see the *JUNOS System Basics and Services Command Reference*.

## Configuring Address-Assignment Pools

The address-assignment pool feature supports subscriber management functionality by enabling you to create address pools that can be shared by different client applications. For example, multiple client applications, such as DHCP, can use an address-assignment pool to provide addresses for their particular clients. Client applications can acquire addresses for either authenticated or unauthenticated clients.

Address-assignment pools support both dynamic and static address assignment. In dynamic address assignment, a client is automatically assigned an address from the address-assignment pool. In static address assignment, you reserve an address that is then always used by a particular client. Addresses that are reserved for static assignment are removed from the dynamic address pool and cannot be assigned to other clients.

Address-assignment pools support named address ranges, which are subsets of the overall address range. A client application can use named ranges to manage address assignment based on client-specific criteria. For example, you might create a named range that is based on a specific DHCP option 82 value. Then, when a DHCP client request matches the specified option 82 value, an address from the specified range

is assigned to the client. The address lease also contains the DHCP configuration options specified in the dhcp-attributes statement.

**NOTE:** You cannot use address-assignment pools with the J-series DHCP server. Also, address-assignment pools are completely separate from L2TP address pools, which you create with the address-pool statement at the [edit access] hierarchy level, and NAT pools, which you create with the pool statement at the [edit services nat] hierarchy level.

To configure an address-assignment pool, include the address-assignment statement at the [edit access] hierarchy level. Include the dhcp-attributes statement to enable DHCP support for the address-assignment pool.

```
[edit access]
address-assignment {
   pool pool-name family inet {
      network address-or-prefix</subnet-mask>;
      range name {
         low lower-limit high upper-limit;
      }
      host hostname {
         hardware-address mac-address;
         ip-address ip-address;
      }
      dhcp-attributes {
         option-match {
            option-82 {
               circuit-id value range named-range;
               remote-id value range named-range;
            }
         }
         boot-file filename;
         boot-server (address | hostname);
         domain-name domain-name;
         grace-period seconds;
         maximum-lease-time seconds;
         name-server [ server-names ];
         netbios-node-type node-type;
         option {
            [ (id-number option-type option-value)
            (id-number array option-type option-value) ];
         }
         router [ router-names ];
         tftp-server address;
         wins-server [ server-names ];
      }
   }
}
```

The following sections describe the configuration of the address-assignment pool feature:



### License Requirements

The address-assignment pool feature is part of the JUNOS Subscriber Management Feature Pack license. You must install and properly configure the license to meet the requirements for using the address-assignment pool feature.

For complete information about the JUNOS software licenses, see the "Installing and Managing JUNOS Licenses" chapter of the *JUNOS Software Installation and Upgrade Guide*.

### Configuring the Pool Name and Network Address

To configure an address-assignment pool, include the following mandatory statements at the [edit access] hierarchy level:

```
[edit access]
address-assignment {
   pool pool-name family inet {
      network address-or-prefix</subnet-mask>;
   }
```

The address-assignment pool definition must include the pool name and the network statement. The network statement specifies the network address and prefix length for the addresses in the pool.

The following is an example of an address-assignment pool definition:

```
[edit access]
address-assignment {
   pool isp_1 family inet {
   network 192.168.0.0/16;
```

### Configuring a Named Address Range for Dynamic Address Assignment

Optionally, you can configure multiple named subsets of addresses within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, use the range statement at the [edit access address-assignment pool *pool-name* family inet] hierarchy level to identify the range and configure the lower and upper address boundaries of the range:

```
range name {
    low lower-limit high upper-limit;
}
```

### Configuring Static Address Assignment

You can optionally create a static binding by reserving a specific address for a particular client. When you reserve an address, that address is removed from the address-assignment pool so that it is not assigned to another client. To configure a static address assignment, use the host statement at the [edit access address-assignment pool *pool-name* family init] hierarchy level to identify the client and create a binding between the client MAC address and the assigned IP address:

```
host hostname {
    hardware-address mac-address;
    ip-address ip-address;
}
```

The following is an example of a static binding configuration. This configuration specifies that the client with MAC address 90:00:00:01:00:01 is always assigned IP address 192.168.44.12.

```
host svale6.boston.net {
    hardware-address 90:00:00:01:00:01;
    ip-address 192.168.44.12;
}
```

### Configuring DHCP Client-Specific Attributes

Use the address-assignment pool feature to include application-specific attributes when clients obtain an address. The client application, such as DHCP, uses the attributes to determine how addresses are assigned, and to also provide optional application-specific characteristics to the client. For example, the DHCP application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCP specifies additional DHCP attributes such as the boot-file that the client uses, the lease grace period, and the maximum lease time.

Use the dhcp-attributes statement at the [edit access address-assignment pool *pool-name* family inet] hierarchy level to configure client-specific attributes for DHCP clients. Table 39 on page 461 describes the DHCP attributes.

```
dhcp-attributes {
    option-match {
        option-82 {
            circuit-id value range named-range;
            remote-id value range named-range;
        }
    }
    boot-file filename;
    boot-server (address | hostname);
    domain-name domain-name;
    grace-period seconds;
    maximum-lease-time seconds;
```

```
    name-server [ server-names ];
    netbios-node-type node-type;
    option {
      [ (id-number option-type option-value)
      (id-number array option-type option-value) ];
    }
    router [ router-names ];
    tftp-server address;
    wins-server [ server-names ];
}
```

**Table 39: DHCP-Attributes Statements**

| Statement | Description | Corresponding DHCP Option |
|---|---|---|
| boot-file | Boot filename advertised to the client, and used by the client to complete configuration. | 67 |
| boot-server | Boot server containing the boot file. | 66 |
| domain-name | Domain in which clients search for a DHCP server host. | 15 |
| grace-period | Grace period offered with the lease. | none |
| option-match | Maps option 82 value to named address range. | none |
| maximum-lease-time | Maximum lease time allowed by the DHCP server. | 51 |
| name-server | IP address of domain name server. | 6 |
| netbios-node-type | NetBIOS node type. | 46 |
| option | User-defined options. | – |
| router | IP address for routers on the subnetwork. | 3 |
| tftp-server | Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file. | 150 |
| wins-server | IP address of the Windows NetBIOS name server. | 44 |

### *Example: Configuring an Address-Assignment Pool*

This section shows a sample address-assignment pool configuration. The configuration includes the dhcp-attributes statement, indicating that the pool is used for DHCP clients.

```
[edit access]
address-assignment {
  pool isp_1 family inet {
    network 192.168.0.0/16;
    range southeast {
      low 192.168.102.2 high 192.168.102.254;
```

```
        }
        range northeast {
            low 192.168.119.2 high 192.168.119.250;
        }
        host svale6.boston.net {
        hardware-address 90:00:00:01:00:01;
        ip-address 192.168.44.12;
    }
    dhcp-attributes {
        option-match {
            option-82 {
                circuit-id fiber range northeast;
            }
            option-82 {
                circuit-id cable_net range southeast;
            }
        }
        boot-file boot.client;
        boot-server 192.168.200.100;
        grace-period 3600;
        maximum-lease-time 18000;
        netbios-node-type p-node;
    }
    router 192.168.44.44 192.168.44.45;
    }
}
```

This example creates address-assignment pool isp-1, which contains two named address ranges, southeast and northeast. The address-assignment pool also contains a static binding for client host sval6.boston.net. If the option 82 circuit-id entry matches the string fiber, then DHCP assigns the client an address from the northeast range. If the option 82 circuit-id matches the string cable_net, DHCP assigns an address from the southeast range.

## Tracing Address-Assignment Pool Processes

To trace address-assignment pool processes, you can specify flags in the traceoptions statement at the [edit system processes general-authentication-service] hierarchy level. The default tracing behavior is the following:

- Important events are logged in a file called authd located in the /var/log directory.
- When the file authd reaches 128 kilobytes (KB), it is renamed authd.0, then authd.1, and so on, until there are 3 trace files. Then the oldest trace file (authd2. is overwritten. For more information about how log files are created, see the *JUNOS System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory (/var/log) in which trace files are located. However, you can customize the other trace file settings by including the following statements at the [edit system processes general-authentication-service] hierarchy level:

```
[edit system processes general-authentication-service]
traceoptions {
```

```
    file filename {
        files number;
        size maximum-file-size;
        world-readable | no-world-readable;
        match regex;
    }
    flag address-assignment;
    flag all;
    flag configuration;
    flag framework;
    flag ldap;
    flag local-authentication;
    flag radius;
}
```

These options are described in the following sections:

- Configuring the Address-Assignment Pool Trace Log Filename on page 463
- Configuring the Number and Size of Address-Assignment Pool Processes Log Files on page 463
- Configuring Access to the Log File on page 464
- Configuring a Regular Expression for Lines to Be Logged on page 464
- Configuring the Trace on page 464

### Configuring the Address-Assignment Pool Trace Log Filename

By default, the name of the file that records trace output for address-assignment pools is authd. You can specify a different name by including the file statement at the [edit system processes general-authentication-service] hierarchy level:

```
[edit system processes general-authentication-service traceoptions]
file filename;
```

### Configuring the Number and Size of Address-Assignment Pool Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed *filename*.0, then *filename*.1, and so on, until there are 3 trace files. Then the oldest trace file (*filename*.2) is overwritten.

You can configure the limits on the number and size of trace files by including the following statement at the [edit system processes general-authentication-service traceoptions] hierarchy level:

```
[edit system processes general-authentication-service traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (*filename*) reaches 2 MB, *filename* is renamed *filename*.0, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename*.0 is renamed *filename*.1 and *filename* is renamed *filename*.0. This process repeats until there are 20 trace files. Then the oldest file (*filename*.19) is overwritten by the newest file (*filename*.0).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

### Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the file world-readable statement at the [edit system processes general-authentication-service traceoptions] hierarchy level:

```
[edit system processes general-authentication-service traceoptions]
file world-readable;
```

To explicitly set the default behavior, include the file no-world-readable statement at the [edit system processes general-authentication-service traceoptions] hierarchy level:

```
[edit system processes general-authentication-service traceoptions (Address-Assignment
   Pool)]
file no-world-readable;
```

### Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the [edit system processes general-authentication-service file *filename*] hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system processes general-authentication-service traceoptions]
file filename match regex;
```

### Configuring the Trace

By default, only important events are logged. You can configure the trace operations to be logged by including the following statements at the [edit system <process-name> traceoptions] hierarchy level:

```
[edit system <process-name>traceoptions]
flag {
   address-assignment;
   all;
   configuration;
   framework;
   ldap;
   local-authentication;
   no-remote-trace;
   radius;
}
```

You can specify the following access tracing flags:

- address-assignment—All address-assignment events
- all—All tracing operations
- configuration—Configuration events
- framework—Authentication framework events
- ldap—LDAP authentication events local-authentication
- local-authentication—Local authentication events
- no-remote-trace—Disable remote tracing for a specific process
- radius—RADIUS authentication events

Chapter 14

# Summary of Access Configuration Statements

The following sections explain each of the access configuration statements. The statements are organized alphabetically.

## accounting

**Syntax**

```
accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    order [ accounting-method ];
    statistics (time);
    update-interval minutes;
}
```

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.

The remaining statements are explained separately.

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## accounting-order

**Syntax** accounting-order radius;

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** Statement introduced in JUNOS Release 8.0

**Description** Enable RADIUS accounting for an L2TP profile.

**Options** radius—Use RADIUS accounting method.

**Usage Guidelines** See "Configuring the Accounting Order" on page 421.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## accounting-port

**Syntax** accounting-port *port-number*;

**Hierarchy Level** [edit access radius-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the port number on which to contact the accounting server.

**Options** *port-number*—The port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).

**Usage Guidelines** See "Configuring RADIUS Authentication for L2TP" on page 433.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## accounting-server

**Syntax** accounting-server [ *ip-address* ];

**Hierarchy Level** [edit access profile *profile-name* radius]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify a list of the RADIUS accounting servers used to for accounting for DHCP, L2TP, and PPP clients.

**Options** *ip-address*—The IP version 4 (IPv4) address.

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## accounting-session-id-format

**Syntax** accounting-session-id-format (decimal | description);

**Hierarchy Level** [edit access profile *profile-name* radius options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the format the router uses to identify the accounting session.

**Options** decimal—Use the decimal format.

description—Use the generic format, in the form jnpr *interface-specifier*:*subscriber-session-id*.
**Default:** decimal

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## accounting-stop-on-access-deny

**Syntax** accounting-stop-on-access-deny;

**Hierarchy Level** [edit access profile *profile-name* accounting]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure RADIUS accounting to send an Acct-Stop message when the AAA server denies a client access.

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## accounting-stop-on-failure

**Syntax** accounting-stop-on-failure;

**Hierarchy Level** [edit access profile *profile-name* accounting]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access.

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## address

**Syntax** address *address-or-prefix*;

**Hierarchy Level** [edit access address-pool *pool-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the IP address or prefix value for clients.

**Options** *address-or-prefix*—An address or prefix value.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the Address Pool" on page 414.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## address-assignment

**Syntax**

```
address-assignment {
    pool pool-name family inet {
        network address-or-prefix</subnet-mask>;
        range range-name {
            low lower-limit high upper-limit;
        }
        host hostname {
            hardware-address mac-address;
            ip-address ip-address;
        }
        dhcp-attributes {
            [protocol-specific attributes]
        }
    }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure address-assignment pools that can be used by different client applications.

**Options** *pool-name*—Name assigned to an address-assignment pool.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring Address-Assignment Pools” on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## address-pool

**Syntax**
```
address-pool pool-name {
    address address-or-prefix;
    address-range <low lower-limit> <high upper-limit>;
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Allocate IP addresses for clients.

**Options** *pool-name*—Name assigned to an address pool.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the Address Pool" on page 414.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## address-range

**Syntax**
```
address-range <low lower-limit> <upper upper-limit>;
```

**Hierarchy Level** [edit access address-pool *pool-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the address range.

**Options**
- low *lower-limit*—The lower limit of an address range.
- high *upper-limit*—The upper limit of an address range.

**Usage Guidelines** See "Configuring the Address Pool" on page 414.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## allowed-proxy-pair

**Syntax**

```
allowed-proxy-pair {
    remote remote-proxy-address local local-proxy-address;
}
```

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Specify the network address of the local and remote peer associated with an IKE access profile.

**Options** remote *remote-proxy-address*—Network address of the remote peer.

local *local-proxy-address*—Network address of the local peer.

Default: remote 0.0.0.0/0 local 0.0.0.0/0

**Usage Guidelines** See "Configuring an Internet Key Exchange (IKE) Access Profile" on page 441.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## attributes

**Syntax**

```
attributes {
    ignore {
        framed-ip-netmask;
        input-filter;
        logical-system-routing-instance;
        output-filter;
    }
    exclude
        accounting-authentic [ accounting-on | accounting-off ];
        accounting-delay-time [ accounting-on | accounting-off ];
        accounting-session-id [ access-request | accounting-on | accounting-off |
            accounting-stop ];
        accounting-terminate-cause [ accounting-off ];
        called-station-id [ access-request | accounting-start | accounting-stop ];
        calling-station-id [ access-request | accounting-start | accounting-stop ];
        class [ accounting-start | accounting-stop ];
        dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
        dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
        output-filter [ accounting-start | accounting-stop ];
        event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop ];
        framed-ip-address [ accounting-start | accounting-stop ];
        framed-ip-netmask [ accounting-start | accounting-stop ];
        input-filter [ accounting-start | accounting-stop ];
        input-gigapackets [ accounting-stop ];
        input-gigawords [ accounting-stop ];
        interface-description [ access-request | accounting-start | accounting-stop ];
        nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |
            accounting-stop ];
        nas-port [ access-request | accounting-start | accounting-stop ];
        nas-port-id [ access-request | accounting-start | accounting-stop ];
        nas-port-type [ access-request | accounting-start | accounting-stop ];
        output-gigapackets [ accounting-stop ];
        output-gigawords [ accounting-stop ];
    }
}
```

**Hierarchy Level** [edit access profile *profile-name* radius]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify how the router processes RADIUS attributes.

The statements are explained separately.

**Usage Guidelines** See “Configuring How RADIUS Attributes Are Used” on page 448.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## authentication-order

**Syntax** authentication-order [ *authentication-methods* ];

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Set the order in which the JUNOS software tries different authentication methods when verifying that a client can access the router. For each login attempt, the software tries the authentication methods in order, from first to last.

**Options** radius—Verify the client using RADIUS authentication services.

password—Verify the client using the information configured at the [edit access profile *profile-name* client *client-name*] hierarchy level.

**Usage Guidelines** See "Example: CHAP Authentication with RADIUS" on page 406 and "Configuring the Authentication Order" on page 420.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## authentication-server

**Syntax** authentication-server [ *ip-address* ];

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients.

**Options** *ip-address*—The IPv4 address.

**Usage Guidelines** See "Configuring RADIUS Parameters" on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## boot-file

**Syntax** boot-file *filename*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup. This is equivalent to DHCP option 67.

**Options** *filename*—The location of the boot file on the boot server. The filename can include a pathname.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** boot-server

## boot-server

**Syntax** boot-server (*address* | *hostname*);

**Hierarchy Level** [edit access address-assignment pool *pool-name* dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup. This is equivalent to DHCP option 66.

**Options**
- *address*—The IPv4 address of a boot server.
- *hostname*—The fully qualified hostname of a boot server.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** boot-file

## cell-overhead

**Syntax** cell-overhead;

**Hierarchy Level** [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced in JUNOS Release 8.3.

**Description** Configure the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping on the IQ2 PIC.

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## chap-secret

**Syntax** chap-secret *chap-secret*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the CHAP secret key associated with a peer.

**Options** *chap-secret*—The secret key associated with a peer.

**Usage Guidelines** See "Configuring the CHAP Secret" on page 423.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## circuit-id

**Syntax** circuit-id *value* range *named-range*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* dhcp-attributes option-matchoption-82]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure the address-assignment pool named-range to use for a particular option 82 Agent Circuit ID value.

**Options**
- circuit-id *value*—The string for the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) in DHCP packets.
- range *named-range*—The name of the address-assignment pool range to use.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## client

**Syntax**

```
client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    ike {
        allowed-proxy-pair {
            remote remote-proxy-address local local-proxy-address;
        }
        pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
        ike-policy policy-name;
        interface-id string-value;
    }
    l2tp {
        interface-id interface-id;
        lcp-renegotiation;
        local-chap;
        maximum-sessions-per-tunnel number;
        multilink {
            drop-timeout milliseconds;
            fragmentation-threshold bytes;
        }
        ppp-authentication (chap | pap);
        ppp-profile profile-name;
        shared-secret shared-secret;
    }
    pap-password pap-password;
    ppp {
        cell-overhead;
        encapsulation-overhead bytes;
        framed-ip-address ip-address;
        framed-pool framed-pool;
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
    }
    user-group-profile profile-name;
}
```

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the peer identity.

**Options** *client-name*—A peer identity.

The other options are explained separately.

**Usage Guidelines** See "Configuring the Client" on page 421.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## dhcp-attributes

**Syntax**

```
dhcp-attributes {
   option-match {
      option-82 {
         circuit-id value range named-range;
         remote-id value range named-range;
      }
   }
   boot-file filename;
   boot-server (address | hostname);
   domain-name domain-name;
   grace-period seconds;
   maximum-lease-time seconds;
   name-server [ server-names ];
   netbios-node-type node-type;
   option {
      [ (id-number option-type option-value)
      (id-number array option-type option-value) ];
   }
   router [ router-names ];
   tftp-server address;
   wins-server [ server-names ];
}
```

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure address pools that can be used by different client applications.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## domain-name

**Syntax** domain-name *domain-name*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.

**Options** *domain-name*—Name of the domain.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## drop-timeout

**Syntax** drop-timeout *milliseconds*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name* l2tp multilink]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the drop timeout for a multilink bundle.

**Options** *milliseconds*—Number of milliseconds for the timeout that is associated with the first fragment on the reassembly queue. If the timeout expires before all the fragments have been collected, the fragments at the beginning of the reassembly queue are dropped. If the drop timeout is not specified, the JUNOS software holds on to the fragments. (Fragments may still be dropped if the multilink reassembly algorithm determines that another fragment belonging to the packet on a reassembly queue has been lost.)

**Usage Guidelines** See "Configuring L2TP Properties for a Profile" on page 424.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## encapsulation-overhead

**Syntax** encapsulation-overhead *bytes*;

**Hierarchy Level** [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced in JUNOS Release 8.3.

**Description** Configure the encapsulation overhead for class-of-service calculations.

**Options** *bytes*—The number of bytes used as encapsulation overhead for the session.

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ethernet-port-type-virtual

**Syntax** ethernet-port-type-virtual;

**Hierarchy Level** [edit access profile *profile-name* radius options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specifies the physical port type the router uses to authenticate clients. The port type is passed in RADIUS attribute 61 (NAS-Port-Type). This statement specifies a port type of virtual; by default the router passes a port type of ethernet in RADIUS attribute 61.

**Usage Guidelines** See "Configuring RADIUS Parameters" on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## exclude

**Syntax**

```
exclude {
    accounting-authentic [ accounting-on | accounting-off ];
    accounting-delay-time [ accounting-on | accounting-off ];
    accounting-session-id [ access-request | accounting-on | accounting-off | accounting-stop
        ];
    accounting-terminate-cause [ accounting-off ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    class [ accounting-start | accounting-stop ];
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
    output-filter [ accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop
        ];
    framed-ip-address [ accounting-start | accounting-stop ];
    framed-ip-netmask [ accounting-start | accounting-stop ];
    input-filter [ accounting-start | accounting-stop ];
    input-gigapackets [ accounting-stop ];
    input-gigawords [ accounting-stop ];
    interface-description [ access-request | accounting-start | accounting-stop ];
    nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |
        accounting-stop ];
    nas-port [ access-request | accounting-start | accounting-stop ];
    nas-port-id [ access-request | accounting-start | accounting-stop ];
    nas-port-type [ access-request | accounting-start | accounting-stop ];
    output-gigapackets [ accounting-stop ];
    output-gigawords [ accounting-stop ];
}
```

**Hierarchy Level** [edit access profile *profile-name* radius attributes]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the router to exclude the specified attributes from the specified type of RADIUS message.

Not all attributes are available in all types of RADIUS messages. By default, the router includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages.

**Options** RADIUS attribute type—RADIUS attribute or Juniper Networks VSA number and name.

- accounting-authentic—RADIUS attribute 45, Acct-Authentic.
- accounting-delay-time—RADIUS attribute 41, Acct-Delay-Time.
- accounting-session-id—RADIUS attribute 44, Acct-Session-Id.
- accounting-terminate-cause—RADIUS attribute 49, Acct-Terminate-Cause.
- called-station-id—RADIUS attribute 30, Called-Station-Id.

- calling-station-id—RADIUS attribute 31, Calling-Station-Id.
- class—RADIUS attribute 25, Class.
- dhcp-gi-address—Juniper VSA 26-57, DHCP-GI-Address.
- dhcp-mac-address—Juniper VSA 26-56, DHCP-MAC-Address.
- event-timestamp—RADIUS attribute 55, Event-Timestamp.
- framed-ip-address—RADIUS attribute 8, Framed-IP-Address.
- framed-ip-netmask—RADIUS attribute 9, Framed-IP-Netmask.
- input-filter—Juniper VSA 26-10, Ingress-Policy-Name.
- input-gigapackets—Juniper VSA 26-42, Acct-Input-Gigapackets.
- input-gigawords—RADIUS attribute 52, Acct-Input-Gigawords.
- interface-description—Juniper VSA 26-53, Interface-Desc.
- nas-identifier—RADIUS attribute 32, NAS-Identifier.
- nas-port—RADIUS attribute 5, NAS-Port.
- nas-port-id—RADIUS attribute 87, NAS-Port-Id.
- nas-port-type—RADIUS attribute 61, NAS-Port-Type.
- output-filter—Juniper VSA 26-11, Egress-Policy-Name.
- output-gigapackets—Juniper VSA 25-43, Acct-Output-Gigapackets.
- output-gigawords—RADIUS attribute 53, Acct-Output-Gigawords.

RADIUS message type

- access-request—RADIUS Access-Accept messages.
- accounting-off—RADIUS Accounting-Off messages.
- accounting-on—RADIUS Accounting-On messages.
- accounting-start—RADIUS Accounting-Start messages.
- accounting-stop—RADIUS Accounting-Stop messages.

**Usage Guidelines** See “Configuring RADIUS Parameters” on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## fragmentation-threshold

**Syntax** fragmentation-threshold *bytes*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name* l2tp multilink]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the fragmentation threshold for multilink bundle.

**Options** *bytes*—The maximum number of bytes in a packet. If a packet exceeds the fragmentation threshold, the JUNOS software fragments it into two or more multilink fragments.

**Usage Guidelines** See "Configuring L2TP Properties for a Profile" on page 424. See also multilink.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## framed-ip-address

**Syntax** framed-ip-address *address*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify a framed IP address.

**Options** *address*—The IP version 4 (IPv4) prefix.

**Usage Guidelines** See "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## framed-pool

**Syntax** framed-pool *framed-pool*;

**Hierarchy Level** [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the address pool.

**Options** *framed-pool*—References a configured address pool.

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## grace-period

**Syntax** grace-period *seconds*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure the amount of time that the client retains the address lease after the lease expires. The address cannot be reassigned to another client during the grace period.

**Options** *seconds*—Number of seconds the lease is retained.
**Range:** 0 through 4,294,967,295 seconds
**Default:** 0 (no grace period)

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## group-profile

See the following sections:

- group-profile (Group Profile) on page 488
- group-profile (Profile) on page 489

### *group-profile (Group Profile)*

**Syntax**

```
group-profile profile-name {
    l2tp {
        interface-id interface-id;
        lcp-renegotiation;
        local-chap;
        maximum-sessions-per-tunnel number;
    }
    ppp {
        cell-overhead;
        encapsulation-overhead bytes;
        framed-pool pool-id;
        idle-timeout seconds;
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
    }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the group profile.

**Options** *profile-name*—Name assigned to the group profile.

The other options are explained separately.

**Usage Guidelines** See "Configuring the Group Profile" on page 415, "Configuring L2TP for a Group Profile" on page 416, "Configuring the PPP Attributes for a Group Profile" on page 417.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *group-profile (Profile)*

**Syntax** group-profile *profile-name*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Associate a group profile with a client.

**Options** *profile-name*—(Optional) Name assigned to the group profile.

**Usage Guidelines** See "Referencing the Group Profile" on page 424.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## hardware-address

**Syntax** hardware-address *mac-address*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet host *hostname*]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify the MAC address of the client. This is the hardware address that identifies the client on the network.

**Options** *mac-address*—The MAC address of the client.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## host

**Syntax**
```
host hostname {
    hardware-address mac-address;
    interface-id ip-address;
}
```

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure a static binding for the specified client.

**Options** *hostname*—Name of the client.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## idle-timeout

**Syntax**
```
idle-timeout seconds;
```

**Hierarchy Level** [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the idle timeout for a user.

**Options** *seconds*—The number of seconds a user can remain idle before the session is terminated.
**Range:** 0 through 4,294,967,295 seconds
**Default:** 0

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ignore

**Syntax**

```
ignore {
    framed-ip-netmask;
    input-filter;
    logical-system-routing-instance;
    output-filter;
}
```

**Hierarchy Level** [edit access profile *profile-name* radius attributes]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the router to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router processes the attributes it receives from the external server.

**Options** framed-ip-netmask—Framed-IP-Netmask (RADIUS attribute 9).

input-filter—Ingress-Policy-Name (VSA 26-10).

logical-system-routing-instance—Virtual-Router (VSA 26-1).

output-filter—Egress-Policy-Name (VSA 26-11).

**Usage Guidelines** See “Configuring RADIUS Parameters” on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ike

**Syntax**

```
ike {
    allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
    }
    pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
    ike-policy policy-name;
    interface-id string-value;
}
```

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]

**Release Information** Statement introduced in JUNOS Release 7.4.
ike-policy statement introduced in JUNOS Release 8.2

**Description** Configure an IKE access profile.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring an Internet Key Exchange (IKE) Access Profile" on page 441.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ike-policy

**Syntax** ike-policy *policy-name*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name* ike]

**Release Information** Statement introduced in JUNOS Release 8.2.

**Description** Specify the IKE policy used to authenticate dynamic peers during IKE negotiation.

**Options** *policy-name*—The name of an IKE policy configured at the [edit services ipsec-vpn ike policy *policy-name*] hierarchy level. The IKE policy defines either the local digital certificate or the pre-shared key used for IKE authentication with dynamic peers. For more information about how to configure the IKE policy, see the *JUNOS Services Interfaces Configuration Guide*.

**Usage Guidelines** See "Configuring an Internet Key Exchange (IKE) Access Profile" on page 441.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** *JUNOS Services Interfaces Configuration Guide* and *JUNOS Feature Guide*

## immediate-update

**Syntax** immediate-update;

**Hierarchy Level** [edit access profile *profile-name* accounting]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the router to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.

**Usage Guidelines** See "Configuring RADIUS Parameters" on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## initiate-dead-peer-detection

**Syntax** initiate-dead-peer-detection;

**Hierarchy Level** [edit access profile *profile-name* client *client-name* ike]

**Release Information** Statement introduced in JUNOS Release 8.3.

**Description** Detect inactive peers on dynamic IPSec tunnels.

**Usage Guidelines** See "Configuring an Internet Key Exchange (IKE) Access Profile" on page 441.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## interface-description-format

**Syntax** interface-description-format (adapter | sub-interface);

**Hierarchy Level** [edit access profile *profile-name* radius options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specifies the information that is included in or omitted from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the router includes both the subinterface and the adapter in the interface description.

**Options** adapter—Specifies the adapter.

sub-interface—Specifies the subinterface.

**Usage Guidelines** See "Configuring RADIUS Parameters" on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## interface-id

**Syntax** interface-id *interface-id*;

**Hierarchy Level** [edit access group-profile *profile-name* l2tp],
[edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ike],
[edit access profile *profile-name* client *client-name* l2tp],
[edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the interface identifier.

**Options** *interface-id*—The identifier for the interface representing a Layer 2 Tunneling Protocol (L2TP) session configured at the [edit interfaces *interface-name* unit *local-unit-number* dial-options] hierarchy level. For more information about the interface ID, see the *JUNOS Services Interfaces Configuration Guide*.

**Usage Guidelines** See "Configuring L2TP for a Group Profile" on page 416, "Configuring the PPP Attributes for a Group Profile" on page 417, "Configuring L2TP Properties for a Profile" on page 424, "Configuring the PPP Properties for a Profile" on page 428, and "Configuring an Internet Key Exchange (IKE) Access Profile" on page 441.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ip-address

**Syntax** ip-address *ip-address*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet host *hostname*]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify the reserved IP address assigned to the client.

**Options** *ip-address*—The IP version 4 (IPv4) address.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## keepalive

**Syntax** keepalive *seconds*;

**Hierarchy Level** [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the keepalive interval for an L2TP tunnel.

**Options** *seconds*—The time period that must elapse before the JUNOS software checks the status of the Point-to-Point Protocol (PPP) session by sending an echo request to the peer.
**Range:** 0 through 32,767 seconds

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## l2tp

See the following sections:



### *l2tp (Group Profile)*

**Syntax**

```
l2tp {
    interface-id interface-id;
    lcp-renegotiation;
    local-chap;
    maximum-sessions-per-tunnel number;
}
```

**Hierarchy Level** [edit access group-profile *profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the Layer 2 Tunneling Protocol for a group profile.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring L2TP for a Group Profile” on page 416.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *l2tp (Profile)*

**Syntax**
```
l2tp {
    interface-id interface-id;
    lcp-renegotiation;
    local-chap;
    maximum-sessions-per-tunnel number;
    multilink {
        drop-timeout milliseconds;
        fragmentation-threshold bytes;
    }
    ppp-authentication (chap | pap);
    ppp-profile profile-name;
    shared-secret shared-secret;
}
```

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the L2TP properties for a profile.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring L2TP Properties for a Profile" on page 424.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## lcp-renegotiation

**Syntax** lcp-renegotiation;

**Hierarchy Level** [edit access group-profile *profile-name* l2tp],
[edit access profile *profile-name* client *client-name* l2tp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the L2TP network server (LNS) so it renegotiates the link control protocol (LCP) with the PPP client.

**Usage Guidelines** See "Configuring L2TP for a Group Profile" on page 416 and "Configuring L2TP Properties for a Profile" on page 424.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## local-chap

**Syntax** local-chap;

**Hierarchy Level** [edit access group-profile *profile-name* l2tp],
[edit access profile *profile-name* client *client-name* l2tp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the JUNOS software so that the LNS ignores proxy authentication attribute-value pairs (AVPs) from the L2TP access concentrator (LAC) and reauthenticates the PPP client using a Challenge Handshake Authentication Protocol (CHAP) challenge. When you do this, the LNS directly authenticates the PPP client.

**Usage Guidelines** See "Configuring L2TP for a Group Profile" on page 416 and "Configuring L2TP Properties for a Profile" on page 424.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## maximum-lease-time

**Syntax** maximum-lease-time *seconds*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify the maximum length of time, in seconds, that the lease is held for a client if the client does not renew the lease. This is equivalent to DHCP option 51.

**Options** *seconds*—The maximum number of seconds the lease can be held.
**Range:** 30 through 4,294,967,295 seconds
**Default:** 86,400 (24 hours)

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## maximum-sessions-per-tunnel

**Syntax** maximum-sessions-per-tunnel *number*;

**Hierarchy Level** [edit access group-profile l2tp],
[edit access profile *profile-name* client *client-name* l2tp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the maximum sessions for a Layer 2 tunnel.

**Options** *number*—Maximum number of sessions for a Layer 2 tunnel.

**Usage Guidelines** See "Configuring L2TP for a Group Profile" on page 416 and "Configuring L2TP Properties for a Profile" on page 424.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## multilink

**Syntax**
```
multilink {
    drop-timeout milliseconds;
    fragmentation-threshold bytes;
}
```

**Hierarchy Level** [edit access profile *profile-name* client *client-name* l2tp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the PPP MP for L2TP.

**Options** The statements are explained separately.

**Usage Guidelines** See "Configuring L2TP Properties for a Profile" on page 424.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## name-server

**Syntax** name-server [*server-names* ];

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure one or more Domain Name System (DNS) name servers available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

**Options** *server-names*—IP addresses of the domain name servers, listed in order of preference.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## nas-identifier

**Syntax** nas-identifier *identifier-value*;

**Hierarchy Level** [edit access profile *profile-name* radius options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.

**Options** *identifier-value*—A string in the range from 1 to 64 characters.

**Usage Guidelines** See "Configuring RADIUS Parameters" on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin–control—To add this statement to the configuration.

## nas-port-extended-format

**Syntax**

```
nas-port-extended-format {
    adapter-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
}
```

**Hierarchy Level** [edit access profile *profile-name* radius options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.

**Options**

adapter-width *width*—Number of bits in the adapter field.

port-width *width*—Number of bits in the port field.

slot-width *width*—Number of bits in the slot field.

stacked-vlan-width *width*—Number of bits in the SVLAN ID field.

vlan-width *width*—Number of bits in the VLAN ID field.

**Usage Guidelines** See “Configuring RADIUS Parameters” on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## netbios-node-type

**Syntax** netbios-node-type *node-type*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify the NetBIOS node type. This is equivalent to DHCP option 46.

**Options** *node-type*—You can specify one of the following node types:

- b-node—Broadcast node
- h-node—Hybrid node
- m-node—Mixed node
- p-node—Peer-to-peer node

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## network

**Syntax** network *address-or-prefix</subnet-mask>*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure subnet information for an address-assignment pool.

**Options**

- *address-or-prefix*—IP version 4 address or prefix value.
- *subnet-mask*—Subnet mask.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## option

**Syntax**

```
option {
   [ (id-number option-type option-value)
   (id-number array option-type option-value) ];
}
```

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify user-defined options that are added to client packets.

**Options**

*id-number*—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.

*option-type*—Any of the following types: flag, byte, string, short, unsigned-short, integer, unsigned-integer, or ip-address.

array—An option can include an array of values.

*option-value*—Value associated with an option. The option value must be compatible with the option type (for example, an On or Off value for a flag type).

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level**

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## options

**Syntax**

```
options {
   accounting-session-id-format (decimal | description);
   ethernet-port-type-virtual;
   interface-description-format (adapter | sub-interface);
   nas-identifier identifier-value;
   nas-port-extended-format {
      adapter-width width;
      port-width width;
      slot-width width;
      stacked-vlan-width width;
      vlan-width width;
   }
   override-nas-information;
   revert-interval interval;
   vlan-nas-port-stacked-format;
}
```

**Hierarchy Level** [edit access profile *profile-name* radius]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the options used by RADIUS authentication and accounting servers.

The statements are explained separately.

**Usage Guidelines** See “Configuring RADIUS Parameters” on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## option-82

**Syntax**
```
option-82 {
   circuit-id value range named-range;
   remote-id value range named-range;
}
```

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes option-match]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify the list of option 82 suboption match criteria used to select the named address range used for the client. The server matches the option 82 value in the user PDU to the specified option 82 match criteria and uses the named address range associated with the string.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## option-match

**Syntax**
```
option-match {
   option-82 {
      circuit-id value range named-range;
      remote-id value range named-range;
   }
}
```

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify a list of match criteria used to determine which named address range in the address-assignment pool to use. The extended DHCP local server matches this information to the match criteria specified in the client PDUs. For example, for option 82 match criteria, the server matches the option 82 value in the user PDU to the specified option 82 string and uses the named range associated with the string.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## order

**Syntax** order [*accounting-method*] [*authentication-method*]

**Hierarchy Level** [edit access profile *profile-name* accounting],
[edit access profile *profile-name* authentication]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Set the order in which the JUNOS software tries different accounting or authentication methods for client activity. When a client logs in, the software tries the accounting and authentication methods in the specified order.

**Options** *accounting-method*—One or more accounting methods. When a client logs in, the software tries the accounting methods in the following order, from first to last.

- radius—Use RADIUS accounting.

*authentication-method*—One or more authentication methods. When a client logs in, the software tries the authentication methods in the following order, from first to last.

- none—Do not perform authentication.
- password—Verify the client using the information configured at the [edit access profile *profile-name* client *client-name*] hierarchy level.
- radius—Verify the client using RADIUS authentication services.

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## override-nas-information

**Syntax** override-nas-information;

**Hierarchy Level** [edit access profile *profile-name* radius options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Specify the information that the RADIUS client includes in broadcast accounting packets. By default, AAA broadcast accounting packets include the NAS-IP-Address and NAS-Identifier attributes of the logical-systems *logical-system-name* routing-instance *routing-instance-name* statement that generates the accounting information. This statement configures the RADIUS client to override the default behavior and include RADIUS attribute 4 (NAS-IP-Address) and RADIUS attribute 32 (NAS-Identifier) of the logical-systems *logical-system-name* routing-instance *routing-instance-name* statement that authenticates the client.

**Usage Guidelines** See "Configuring RADIUS Parameters" on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## pap-password

**Syntax** pap-password *password*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the Password Authentication Protocol (PAP) password.

**Options** *password*—PAP password.

**Usage Guidelines** See "Configuring the Password Authentication Protocol Password for an L2TP Profile" on page 427.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## pool

**Syntax** pool *pool-name*;

**Hierarchy Level** [edit access address-assignment]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure the name of an address-assignment pool.

**Options** *pool-name*—The name assigned to the address-assignment pool.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## port

**Syntax** port *port-number*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the port number on which to contact the RADIUS server.

**Options** *port-number*—Port number on which to contact the RADIUS server.
**Default:** 1812 (as specified in RFC 2865)

**Usage Guidelines** See "Configuring RADIUS Authentication for L2TP" on page 433, "Configuring the RADIUS Disconnect Server for L2TP" on page 438, and "Example: CHAP Authentication with RADIUS" on page 406.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ppp

See the following sections:

- ppp (Group Profile) on page 509
- ppp (Profile) on page 510

### *ppp (Group Profile)*

**Syntax**

```
ppp {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-pool framed-pool;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
}
```

**Hierarchy Level** [edit access group-profile *profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure PPP properties for a group profile.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *ppp (Profile)*

**Syntax**
```
ppp {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-ip-address address;
    framed-pool framed-pool;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
}
```

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure PPP properties for a client profile.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ppp-authentication

**Syntax** ppp-authentication (chap | pap);

**Hierarchy Level** [edit access profile *profile-name* client *client-name* l2tp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure PPP authentication.

**Options**
- chap— The Challenge Handshake Authentication Protocol.
- pap— The Password Authentication Protocol.

**Usage Guidelines** See "Configuring L2TP Properties for a Profile" on page 424.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ppp-profile

**Syntax** ppp-profile *profile-name*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name* l2tp]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Specify the profile used to validate PPP session requests through L2TP tunnels.

**Options** profile-name—Identifier for the PPP profile.

**Usage Guidelines** See "Configuring RADIUS Authentication for an L2TP Profile" on page 439.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## pre-shared-key

**Syntax** pre-shared-key (ascii-text *character-string* | hexadecimal *hexadecimal-digits*);

**Hierarchy Level** [edit access profile *profile-name* client *client-name* ike]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation. Specify the key in either ASCII or hexadecimal format.

**Options** ascii-text *character-string*—Authentication key in ASCII format.

hexadecimal *hexadecimal-digits*—Authentication key in hexadecimal format.

**Usage Guidelines** See "Configuring an Internet Key Exchange (IKE) Access Profile" on page 441.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## primary-dns

**Syntax** primary-dns *primary-dns*;

**Hierarchy Level** [edit access group-profile *profile-name* client *client-name* ppp],
[edit access profile *profile-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the primary Domain Name System (DNS) server.

**Options** *primary-dns*—An IPv4 address.

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

## primary-wins

**Syntax** primary-wins *primary-wins*;

**Hierarchy Level** [edit access group-profile *profile-name* client *client-name* ppp],
[edit access profile *profile-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the primary Windows Internet name server.

**Options** *primary-wins*—An IPv4 address.

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## profile

**Syntax**

```
profile profile-name {
    authentication-order [ authentication-methods ];
    accounting {
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        order [ accounting-method ];
        statistics (time);
        update-interval minutes;
    }
    authentication-order [ authentication-method ]
    client client-name {
        chap-secret chap-secret;
        group-profile profile-name;
        ike {
            allowed-proxy-pair {
                remote remote-proxy-address local local-proxy-address;
            }
            pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
            ike-policy policy-name;
            interface-id string-value;
        }
        l2tp {
            interface-id interface-id;
            lcp-renegotiation;
            local-chap;
            maximum-sessions-per-tunnel number;
            multilink {
                drop-timeout milliseconds;
                fragmentation-threshold bytes;
            }
            ppp-authentication (chap | pap);
            ppp-profile profile-name;
            shared-secret shared-secret;
        }
        pap-password pap-password;
        ppp {
            cell-overhead;
            encapsulation-overhead bytes;
            framed-ip-address ip-address;
            framed-pool framed-pool;
            idle-timeout seconds;
            interface-id interface-id;
            keepalive seconds;
            primary-dns primary-dns;
            primary-wins primary-wins;
            secondary-dns secondary-dns;
            secondary-wins secondary-wins;
        }
        user-group-profile profile-name;
    }
    radius {
```

```
    authentication-server [ ip-address ];
    accounting-server [ ip-address ];
    options {
      accounting-session-id-format (decimal | description);
      ethernet-port-type-virtual;
      interface-description-format (adapter | sub-interface);
      nas-identifier identifier-value;
      nas-port-extended-format {
        adapter-width width;
        port-width width;
        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
      }
      override-nas-information;
      revert-interval interval;
      vlan-nas-port-stacked-format;
    }
    attributes {
      ignore {
        framed-ip-netmask;
        input-filter;
        logical-system-routing-instance;
        output-filter;
      }
      exclude
        accounting-authentic [ accounting-on | accounting-off ];
        accounting-delay-time [ accounting-on | accounting-off ];
        accounting-session-id [ access-request | accounting-on | accounting-off |
          accounting-stop ];
        accounting-terminate-cause [ accounting-off ];
        called-station-id [ access-request | accounting-start | accounting-stop ];
        calling-station-id [ access-request | accounting-start | accounting-stop ];
        class [ accounting-start | accounting-stop ];
        dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
        dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
        output-filter [ accounting-start | accounting-stop ];
        event-timestamp [ accounting-on | accounting-off | accounting-start |
          accounting-stop ];
        framed-ip-address [ accounting-start | accounting-stop ];
        framed-ip-netmask [ accounting-start | accounting-stop ];
        input-filter [ accounting-start | accounting-stop ];
        input-gigapackets [ accounting-stop ];
        input-gigawords [ accounting-stop ];
        interface-description [ access-request | accounting-start | accounting-stop ];
        nas-identifier [ access-request | accounting-on | accounting-off | accounting-start
          | accounting-stop ];
        nas-port [ access-request | accounting-start | accounting-stop ];
        nas-port-id [ access-request | accounting-start | accounting-stop ];
        nas-port-type [ access-request | accounting-start | accounting-stop ];
        output-gigapackets [ accounting-stop ];
        output-gigawords [ accounting-stop ];
      }
    }
  }
  radius-server server-address {
```

```
        accounting-port port-number;
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        secret password;
        source-address source-address;
        timeout seconds;
    }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

**Options** *profile-name*—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the Point-to-Point Protocol" on page 405, "Configuring the Profile" on page 419, "Configuring L2TP Properties for a Profile" on page 424, "Configuring the PPP Properties for a Profile" on page 428, and "Managing Subscriber Access" on page 442.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## radius

**Syntax**

```
radius {
    authentication-server [ ip-address ];
    accounting-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        ethernet-port-type-virtual;
        interface-description-format (adapter | sub-interface);
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
        }
        override-nas-information;
        revert-interval interval;
        vlan-nas-port-stacked-format;
    }
    attributes {
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system-routing-instance;
            output-filter;
        }
        exclude
            accounting-authentic [ accounting-on | accounting-off ];
            accounting-delay-time [ accounting-on | accounting-off ];
            accounting-session-id [ access-request | accounting-on | accounting-off |
                accounting-stop ];
            accounting-terminate-cause [ accounting-off ];
            called-station-id [ access-request | accounting-start | accounting-stop ];
            calling-station-id [ access-request | accounting-start | accounting-stop ];
            class [ accounting-start | accounting-stop ];
            dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
            dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
            output-filter [ accounting-start | accounting-stop ];
            event-timestamp [ accounting-on | accounting-off | accounting-start |
                accounting-stop ];
            framed-ip-address [ accounting-start | accounting-stop ];
            framed-ip-netmask [ accounting-start | accounting-stop ];
            input-filter [ accounting-start | accounting-stop ];
            input-gigapackets [ accounting-stop ];
            input-gigawords [ accounting-stop ];
            interface-description [ access-request | accounting-start | accounting-stop ];
            nas-identifier [ access-request | accounting-on | accounting-off | accounting-start
                | accounting-stop ];
            nas-port [ access-request | accounting-start | accounting-stop ];
            nas-port-id [ access-request | accounting-start | accounting-stop ];
            nas-port-type [ access-request | accounting-start | accounting-stop ];
```

```
            output-gigapackets [ accounting-stop ];
            output-gigawords [ accounting-stop ];
        }
    }
}
```

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The statements are explained separately.

**Usage Guidelines** See "Configuring RADIUS Parameters" on page 446.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## radius-disconnect

**Syntax**

```
radius-disconnect {
    client-address {
        secret password;
    }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a disconnect server that listens on a configured User Datagram Protocol (UDP) port for disconnect messages from a configured client and processes these disconnect messages.

**Options** *client-address*—A valid IP address configured on one of the router interfaces.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the RADIUS Disconnect Server for L2TP" on page 438.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## radius-disconnect-port

**Syntax** radius-disconnect-port *port-number*;

**Hierarchy Level** [edit access]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Specify a port number on which to contact the RADIUS disconnect server. Most RADIUS servers use port number 1700.

**Options** *port-number*—The server port to which disconnect requests from the RADIUS client are sent. The L2TP network server, which accepts these disconnect requests, is the server.

**NOTE:** The JUNOS software accepts disconnect requests only from the client address configured at the [edit access radius-disconnect client *client-address*] hierarchy level.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the RADIUS Disconnect Server for L2TP" on page 438.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## radius-server

**Syntax**

```
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry number;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

**Hierarchy Level** [edit access],
[edit access profile *profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure RADIUS for subscriber access management, L2TP, or PPP.

To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

**Options** *server-address*—Address of the RADIUS authentication server.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring RADIUS Authentication for L2TP" on page 433, "Configuring the Point-to-Point Protocol" on page 405, "Configuring RADIUS Authentication" on page 77, and "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## range

**Syntax**
```
range range-name {
    low lower-limit high upper-limit;
}
```

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure a named address range used within an address-assignment pool.

**Options** *range-name*—The name assigned to the range of addresses.

low *lower-limit*—The lower limit of an address range.

high *upper-limit*—The upper limit of an address range.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## remote-id

**Syntax** remote-id *value* range *named-range*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes option-match option-82]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify the address-assignment pool named range to use based on the particular option 82 Agent Remote ID value.

**Options** remote-id *value*—The string for Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) in DHCP packets.

range *named-range*—Name of the address-assignment pool range to use.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## retry

**Syntax** retry *attempts*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Number of times that the router is allowed to attempt to contact a RADIUS authentication or accounting server.

**Options** *attempts*—Number of times that the router is allowed to attempt to contact a RADIUS server.
**Range:** 1 through 10
**Default:** 3

**Usage Guidelines** See "Configuring RADIUS Authentication for L2TP" on page 433 or "Example: CHAP Authentication with RADIUS" on page 406.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** timeout

## revert-interval

**Syntax** revert-interval *interval*;

**Hierarchy Level** [edit access profile *profile-name* radius options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the amount of time the router waits after a server has become unreachable. The router rechecks the connection to the server when the revert-interval expires. If the server is then reachable, it is used in accordance with the order of the server list.

**Options** *interval*—Amount of time to wait.
**Range:** 60 through 4294967295 seconds
**Default:** 3 seconds

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## router

**Syntax** router [ *hostnames* ];

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify a list of the routers located on the client's subnet. This statement is the equivalent of DHCP option 3.

**Options** *hostnames*—IP addresses of the routers.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## routing-instance

**Syntax** routing-instance *routing-instance-name*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the routing instance used to send RADIUS packets to the RADIUS server.

**Options** *routing-instance-name*—Routing instance name.

**Usage Guidelines** See "Configuring the Point-to-Point Protocol" on page 405.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** *JUNOS Network Interfaces Configuration Guide*

## secondary-dns

**Syntax** secondary-dns *secondary-dns*;

**Hierarchy Level** [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the secondary DNS server.

**Options** *secondary-dns*—An IPv4 address.

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## secondary-wins

**Syntax** secondary-wins *secondary-wins*;

**Hierarchy Level** [edit access group-profile *profile-name* ppp],
[edit access profile *profile-name* client *client-name* ppp]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the secondary Windows Internet name server.

**Options** *secondary-wins*—An IPv4 address.

**Usage Guidelines** See "Configuring the PPP Attributes for a Group Profile" on page 417 and "Configuring the PPP Properties for a Profile" on page 428.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## secret

**Syntax** secret *password*;

**Hierarchy Level** [edit access profile *profile-name* radius-server *server-address*],
[edit access radius-disconnect *client-address*],
[edit access radius-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the password to use with the RADIUS server. The secret password used by the local router must match that used by the server.

**Options** *password*—Password to use; can include spaces.

**Usage Guidelines** See "Configuring RADIUS Authentication for L2TP" on page 433, "Configuring the RADIUS Disconnect Server for L2TP" on page 438, and "Example: CHAP Authentication with RADIUS" on page 406.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## shared-secret

**Syntax** shared-secret *shared-secret*;

**Hierarchy Level** [edit access profile *profile-name* client *client-name* l2tp]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure the shared secret.

**Options** *shared-secret*—The shared secret key for authenticating the peer.

**Usage Guidelines** See "Configuring L2TP Properties for a Profile" on page 424.

**Required Privilege Level** admin—To view this statement in the configuration.
admin–control—To add this statement to the configuration.

## source-address

**Syntax** source-address *source-address*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.

**Options** *source-address*—A valid IPv4 address configured on one of the router interfaces. On M-series routers only, the source address can be an IPv6 address and the UDP source port is 514.

**Usage Guidelines** See "Configuring RADIUS Authentication for L2TP" on page 433 or "Example: CHAP Authentication with RADIUS" on page 406.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## statistics

**Syntax** statistics (time);

**Hierarchy Level** [edit access profile *profile-name* accounting]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the router to collect time statistics for the sessions being managed by AAA.

**Options** time—Collect uptime statistics only.

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## tftp-server

**Syntax** tftp-server *ip-address*;

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file. This is equivalent to DHCP option 150.

**Options** *ip-address*—IP address of the TFTP server.

**Usage Guidelines** See "Configuring Address-Assignment Pools" on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## timeout

**Syntax** timeout *seconds*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the amount of time that the local router waits to receive a response from a RADIUS server.

**Options** *seconds*—Amount of time to wait.
**Range:** 1 through 90 seconds
**Default:** 3 seconds

**Usage Guidelines** See "Configuring RADIUS Authentication for L2TP" on page 433 or "Example: CHAP Authentication with RADIUS" on page 406.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## traceoptions

**Syntax**

```
traceoptions {
    file filename <files number> <match regex> <size maximum-file-size> <world-readable
        | no-world-readable>;
    flag all;
    flag authentication;
    flag chap;
    flag configuration;
    flag kernel;
    flag radius;
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure access tracing options.

**Options** file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.
**Range:** 2 through 1000
**Default:** 3 files

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.

- all—All tracing operations
- authentication—All authentication module handling
- chap—All CHAP messages and handling
- configuration—Reading of configuration
- kernel—Send all configuration messages to the kernel
- radius—All RADIUS messages and handling

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches its maximum size,

*trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.
**Syntax:** *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
**Range:** 10 KB through 1 GB
**Default:** 128 KB

world-readable—(Optional) Enable unrestricted file access.

**Usage Guidelines** See "Tracing Access Processes" on page 409.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## update-interval

**Syntax** update-interval *minutes*;

**Hierarchy Level** [edit access profile *profile-name* accounting]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure the amount of time, in minutes, that the router waits before sending a new accounting update.

**Options** *minutes*—Amount of time between updates, in minutes.
**Range:** 15 through 1440 minutes
**Default:** no updates

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## user-group-profile

**Syntax** user-group-profile *profile-name*;

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** (M7i and M10i routers only) Statement introduced before JUNOS Release 7.4.

**Description** Apply a configured PPP group profile to PPP users.

**Options** *profile-name*—Name of a PPP group profile configured at the [edit access group-profile *profile-name*] hierarchy level.

**Usage Guidelines** See "Applying a Configured PPP Group Profile to a Tunnel" on page 429.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## vlan-nas-port-stacked-format

**Syntax** vlan-nas-port-stacked-format;

**Hierarchy Level** [edit access profile *profile-name* radius options]

**Release Information** Statement introduced in JUNOS Release 9.1.

**Description** Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

**Usage Guidelines** See "Using RADIUS Authentication and Accounting for Subscriber Access Management" on page 443.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## wins-server

**Syntax** wins-server [*hostnames* ];

**Hierarchy Level** [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Specify one or more NetBIOS name servers (NBNS) that the client uses to resolve NetBIOS names. This is equivalent to DHCP option 44.

**Options** *server-list*—IP addresses of the NetBIOS name servers, listed in order of preference.

**Usage Guidelines** See “Configuring Address-Assignment Pools” on page 457.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

# Part 4
# Security Services

Chapter 15

# Security Services Overview

The JUNOS software supports Internet Protocol Security (IPSec). This chapter discusses the following topics, which provide background information related to configuring IPSec:



## IPSec Overview

IPSec architecture provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPSec, the JUNOS software also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs).

IPSec also defines a security association and key management framework that can be used with any network layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. IPSec provides secure tunnels between two peers.

For a complete description of the IPSec security suite, see the "IPSec" chapter of the *JUNOS Feature Guide*.

## Security Associations

To use IPSec security services, you create SAs between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPSec. There are two types of SAs: manual and dynamic.

- Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. Manual SAs statically define the Security Parameter Index (SPI) values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.
- Dynamic SAs require additional configuration. With dynamic SAs, you configure IKE first and then the SA. IKE creates dynamic security associations; it negotiates

SAs for IPSec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. This connection is then used to dynamically agree upon keys and other data used by the dynamic IPSec SA. The IKE SA is negotiated first and then used to protect the negotiations that determine the dynamic IPSec SAs.

The JUNOS software implementation of IPSec supports two modes of security (transport and tunnel). For more information about transport and tunnel mode, see "Configuring IPSec Mode" on page 541.

## IKE

IKE is a key management protocol that creates dynamic SAs; it negotiates SAs for IPSec. An IKE configuration defines the algorithms and keys used to establish a secure connection with a peer security gateway.

IKE does the following:

- Negotiates and manages IKE and IPSec parameters
- Authenticates secure key exchange
- Provides mutual peer authentication by means of shared secrets (not passwords) and public keys
- Provides identity protection (in main mode)

IKE occurs over two phases. In the first phase, it negotiates security attributes and establishes shared secrets to form the bidirectional IKE SA. In the second phase, inbound and outbound IPSec SAs are established. The IKE SA secures the exchanges in the second phase. IKE also generates keying material, provides Perfect Forward Secrecy, and exchanges identities.

## IPSec Requirements for JUNOS-FIPS

In a JUNOS-FIPS environment, hardware configurations with two Routing Engines must be configured to use IPSec and a private routing instance for all communications between the Routing Engines. IPSec communication between the Routing Engines and AS II FIPS PICs is also required. For more information about JUNOS-FIPS security, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

Chapter 16

# Security Services Configuration Guidelines

To configure security services, include the following statements at the [edit security] hierarchy level:

```
[edit security]
authentication-key-chains {
    key-chain key-chain-name {
        key key {
            secret secret-data;
            start-time yyyy-mm-dd.hh:mm:ss;
        }
    }
}
certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
        ca-name ca-identity;
        crl file-name;
        encoding (binary | pem);
        enrollment-url url-name;
        file certificate-filename;
        ldap-url url-name;
    }
    enrollment-retry attempts ;
    local certificate-filename {
        certificate-key-string;
        load-key-file key-file-name;
    }
    maximum-certificates number;
    path-length certificate-path-length;
}
ike {
    proposal ike-proposal-name {
        authentication-algorithm (md5 | sha1);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        description description;
        dh-group (group1 | group2);
        encryption-algorithm (3des-cbc | des-cbc | ase-128-cbc | ase-192-cbc |
            ase-256-cbc);
        lifetime-seconds seconds;
```

```
    }
    policy ike-peer-address {
        description description;
        encoding (binary | pem);
        identity identity-name;
        local-certificate certificate-filename;
        local-key-pair private-public-key-file;
        mode (aggressive | main);
        pre-shared-key (ascii-text key | hexadecimal key);
        proposals [ proposal-names ];
    }
}
ipsec {
    security-association {
        manual {
            direction (bidirectional | inbound | outbound) {
                protocol esp;
                spi spi-value;
                encryption {
                    algorithm 3des-cbc;
                    key ascii-text ascii-text-string;
                }
            }
        }
    }
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        description description;
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol (ah | esp | bundle);
    }
    policy ipsec-policy-name {
        description description;
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposals [ proposal-names ];
    }
    security-association sa-name {
        description description;
        dynamic {
            ipsec-policy policy-name;
            replay-window-size (32 | 64);
        }
        manual {
            direction (inbound | outbound | bidirectional) {
                authentication {
                    algorithm (hmac-md5-96 | hmac-sha1-96);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi auxiliary-spi;
                encryption {
                    algorithm (des-cbc | 3des-cbc);
                    key (ascii-text key | hexadecimal key);
                }
```

```
            protocol (ah | esp | bundle);
            spi spi-value ;
          }
        }
        mode (tunnel | transport);
      }
    }
    pki {
      ca-profile ca-profile-name {
        ca-identity ca-identity;
        enrollment {
          url url-name;
          retry number-of-attempts;
          retry-interval seconds;
        }
        revocation-check {
          disable;
          crl {
            disable on-download-failure;
            refresh-interval number-of-hours;
            url {
              url-name;
              password;
            }
          }
        }
      }
    }
    ssh-known-hosts {
      host {
        dsa-key key ;
        rsa-key key ;
        rsa1-key key ;
      }
    }
    traceoptions {
      file filename <files number> < size size>;
      flag all;
      flag database;
      flag general;
      flag ike;
      flag parse;
      flag policy-manager;
      flag routing-socket;
      flag timer;
    }
```

**NOTE:** Most of the configuration statements do not have default values. If you do not specify an identifier for a statement that does not have a default value, you cannot commit the configuration.

For information about IP Security (IPSec) monitoring and troubleshooting, see the *JUNOS System Basics and Services Command Reference*.

This chapter describes how to configure IPSec for the ES PIC, IPSec digital certificates for adaptive services interfaces, and internal IPSec for JUNOS-FIPS. It also describes how to configure miscellaneous security services, including authentication key updates for Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP), SSH host keys for secure copy, and Secure Sockets Layer (SSL) for JUNOScript client applications:



## Configuring IPSec (ES PIC)

IPSec provides a secure way to authenticate senders and encrypt IPv4 and IPv6 traffic between network devices, such as routing platforms and hosts. The following sections show how to configure IPSec for an ES PIC:



The key management process (kmd) provides IPSec authentication services for ES PICs. The key management process starts only when IPSec is configured on the router.

### *Minimum Manual SA Configuration*

To define a manual security association (SA) configuration for an ES PIC, you must include at least the following statements at the [edit security ipsec] hierarchy level:

```
[edit security ipsec]
security-association sa-name {
    manual {
```

```
        direction (inbound | outbound | bidirectional) {
            authentication {
                algorithm (hmac-md5-96 | hmac-sha1-96);
                key (ascii-text key | hexadecimal key);
            }
            encryption {
                algorithm (des-cbc | 3des-cbc);
                key (ascii-text key | hexadecimal key);
            }
            protocol (ah | esp | bundle);
            spi spi-value;
        }
    }
}
```

**NOTE:** You configure a manual SA for AS and MultiServices PICs at the [edit services ipsec-vpn rule *rule-name* term *term-name* then manual] hierarchy level.

For more information, see the "IPSec" chapter of the *JUNOS Feature Guide* and the "IPSec Services Configuration Guidelines" chapter of the *JUNOS Services Interfaces Configuration Guide*.

### *Minimum IKE Configuration*

To define an IKE configuration for an ES PIC, include at least the following statements at the [edit security] hierarchy level:

```
[edit security ike]
proposal ike-proposal-name {
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    dh-group (group1 | group2);
    encryption-algorithm (3des-cbd | des-cbc | ase-128-cbc | ase-192-cbc | ase-256-cbc);
}
policy ike-peer-address {
    proposals [ ike-proposal-names ];
    pre-shared-key (ascii-text key | hexadecimal key);
}
```

**NOTE:** You configure an IKE policy for AS and MultiServices PICs at the [edit services ipsec-vpn ike] hierarchy level.

For more information, see the "IPSec" chapter of the *JUNOS Feature Guide* and the "IPSec Services Configuration Guidelines" chapter of the *JUNOS Services Interfaces Configuration Guide*.

### *Minimum Digital Certificates Configuration for IKE (ES PIC)*

To define a digital certificates configuration for IKE for an encryption interface on M-series and T-series routing platforms, include at least the following statements at the [edit security certificates] and [edit security ike] hierarchy levels:

```
[edit security]
certificates {
    certification-authority ca-profile-name {
        ca-name ca-identity;
        crl filename;
        enrollment-url url-name;
        file certificate-filename;
        ldap-url url-name;
    }
}
ike {
    policy ike-peer-address {
        local-certificate certificate-filename;
        local-key-pair private-public-key-file;
        proposal [ ike-proposal-names ];
    }
    proposal ike-proposal-name {
        authentication-method rsa-signatures;
    }
}
```

### *Configuring Security Associations*

To use IPSec security services, you create an SA between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPSec. You can configure two types of SAs:

- Manual—Requires no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place. For information about how to configure a manual SA, see "Configuring Manual Security Associations" on page 543.
- Dynamic—Specifies proposals to be negotiated with the tunnel peer. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more proposal statements, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer. For information about how to configure a dynamic SA, see "Configuring the ES PIC" on page 567.

**NOTE:** The JUNOS software does not perform a commit check when an SA name referenced in the Border Gateway Protocol (BGP) protocol section is not configured at the [edit security ipsec] hierarchy level.

We recommend that you configure no more than 512 dynamic security associations per ES Physical Interface Card (PIC).

To configure an SA for IPSec for an ES PIC, include the security-association statement at the [edit security ipsec] hierarchy level:

```
[edit security ipsec]
security-association sa-name;
```

This section describes the following topics related to configuring security associations:



**NOTE:** You configure a dynamic SA for the AS and MultiServices PICs at the [edit services ipsec-vpn rule *rule-name* term *term-name* then dynamic], [edit services ipsec-vpn ike], and [edit services ipsec-vpn ipsec] hierarchy levels.

For more information, see the "IPSec" chapter of the *JUNOS Feature Guide* and the "IPSec Services Configuration Guidelines" chapter of the *JUNOS Services Interfaces Configuration Guide*.

## Configuring the Description for an SA

To specify a description for an IPSec SA, include the description statement at the edit security ipsec security-association *sa-name*] hierarchy level:

```
[edit security ipsec security-association sa-name]
description description;
```

## Configuring IPSec Mode

The JUNOS software implementation of IPSec supports two modes of security: transport and tunnel mode. By default, tunnel mode is enabled.

This section discusses the following topics:



### *Configuring Transport Mode*

In transport mode, the data portion of the IP packet is encrypted, but the IP header is not. Transport mode can be used only when the communication endpoint and cryptographic endpoint are the same. Virtual private network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications. You configure manual SAs, and you must configure static values on both ends of the SA.

**NOTE:** When you use transport mode, the JUNOS software supports both BGP and OSPFv3 for manual SAs.

To configure IPSec security for transport mode, include the mode statement with the transport option at the edit security ipsec security-association *sa-name*] hierarchy level:

```
[edit security ipsec security-association sa-name]
mode transport;
```

To apply tunnel mode, you configure manual SAs in transport mode and then reference the SA by name at the [edit protocols bgp] hierarchy level to protect a session with a given peer. For more information about how to reference the configured SA, see the *JUNOS Routing Protocols Configuration Guide*.

**NOTE:** You can configure BGP to establish a peer relationship over encrypted tunnels.

### *Configuring Tunnel Mode*

You use tunnel mode when you use preshared keys with IKE to authenticate peers, or digital certificates with IKE to authenticate peers. In tunnel mode, encryption services are performed on an ES PIC.

When you use preshared keys, you manually configure a preshared key, which must match that of its peer. With digital certificates, each router is dynamically or manually enrolled with a certificate authority (CA). When a tunnel is established, the public keys used for IPsec are dynamically obtained through IKE and validated against the CA certificate. This avoids the manual configuration of keys on routers within the topology. Adding a new router to the topology does not require any security configuration changes to existing routers.

To configure the IPSec in tunnel mode, include the mode statement with the tunnel option at the edit security ipsec security-association *sa-name*] hierarchy level:

```
[edit security ipsec security-association sa-name]
mode tunnel;
```

**NOTE:** Tunnel mode requires the ES PIC.

The JUNOS software supports both both BGP and OSPFv3 in transport mode.

To enable tunnel mode, follow the steps in these sections:

- Configuring Security Associations on page 540
- Configuring an IKE Proposal (Dynamic SAs Only) on page 548
- Configuring the ES PIC on page 567
- Configuring Traffic on page 568

For more information about the ES PIC, see the *JUNOS Services Interfaces Configuration Guide*.

## Configuring Manual Security Associations

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. As a result, peers can communicate only when they all share the same configured options.

To configure the manual IPSec SA for an ES PIC, include the manual statement at the edit security ipsec security-association *sa-name*] hierarchy level:

```
[edit security ipsec security-association sa-name]
manual {
   direction (inbound | outbound | bi-directional) {
      authentication {
         algorithm (hmac-md5-96 | hmac-sha1-96);
         key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi auxiliary-spi-value;
      encryption {
         algorithm (des-cbc | 3des-cbc);
         key (ascii-text key | hexadecimal key);
      }
      protocol (ah | esp | bundle);
      spi spi-value;
   }
}
```

The following sections describe how to configure a manual SA:



### *Configuring the Processing Direction*

The direction statement sets inbound and outbound IPSec processing. If you want to define different algorithms, keys, or security parameter index (SPI) values for each direction, you configure the inbound and outbound options. If you want the same attributes in both directions, use the bidirectional option.

To configure the direction of IPSec processing, include the direction statement and specify the direction at the [edit security ipsec security-association *sa-name* manual] hierarchy level:

```
[edit security ipsec security-association sa-name manual]
direction (inbound | outbound | bidirectional);
```

For sample configurations, see the following sections:

- Example: Configuring Inbound and Outbound Processing on page 544
- Example: Configuring Bidirectional Processing on page 544

### *Example: Configuring Inbound and Outbound Processing*

Define different algorithms, keys, and security parameter index values for each direction:

```
[edit security ipsec security-association sa-name]
manual {
    direction inbound {
        encryption {
            algorithm 3des-cbc;
            key ascii-text 23456789012345678901234;
        }
        protocol esp;
        spi 16384;
    }
    direction outbound {
        encryption {
            algorithm 3des-cbc;
            key ascii-text 123456789012345678901abcd;
        }
        protocol esp;
        spi 24576;
    }
}
```

### *Example: Configuring Bidirectional Processing*

Define the same algorithms, keys, and security parameter index values for each direction:

```
[edit security ipsec security-association sa-name manual]
direction bidirectional {
    authentication {
        algorithm hmac-md5-96;
        key ascii-text 123456789012abcd;
    }
    protocol ah;
    spi 20001;
}
```

### *Configuring the Protocol for a Manual SA*

IPSec uses two protocols to protect IP traffic: Encapsulating Security Payload (ESP) and authentication header (AH). For transport mode SAs, both ESP and AH are supported. The AH protocol is used for strong authentication. The bundle option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

**NOTE:** The AH protocol is supported only on M-series platforms.

To configure the IPSec protocol on an ES PIC, include the protocol statement at the edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bidirectional)] hierarchy level and specify the ah, bundle, or esp option:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bi-directional)]
protocol (ah | bundle | esp);
```

### *Configuring the Security Parameter Index*

An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.

**NOTE:** Each manual SA must have a unique SPI and protocol combination.

Use the auxiliary SPI when you configure the protocol statement to use the bundle option. For more information, see "Configuring the Auxiliary Security Parameter Index" on page 545.

To configure the SPI on an ES PIC, include the spi statement and specify a value (256 through 16,639) at the [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional] hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bidirectional)]
spi spi-value;
```

### *Configuring the Auxiliary Security Parameter Index*

When you configure the protocol statement to use the bundle option, the JUNOS software uses the auxiliary SPI for the ESP and the SPI for the AH.

**NOTE:** Each manual SA must have a unique SPI and protocol combination.

To configure the auxiliary SPI, include the auxiliary-spi statement at the [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)] hierarchy level and set the value to an integer between 256 and 16,639:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bidirectional)]
auxiliary-spi auxiliary-spi-value;
```

### *Configuring the Authentication Algorithm and Key*

To configure an authentication algorithm and key, include the **authentication** statement at the [**edit security ipsec security-association** *sa-name* **manual direction (inbound | outbound | bi-directional)**] hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound
    | bidirectional)]
authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit authenticator value and 96-bit digest.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit authenticator value and a 96-bit digest.

The key can be one of the following:

- **ascii-text** *key*—ASCII text key. With the **hmac-md5-96** option, the key contains
- 16 ASCII characters. With the **hmac-sha1-96** option, the key contains 20 ASCII characters.
- **hexadecimal** *key*—Hexadecimal key. With the **hmac-md5-96** option, the key contains 32 hexadecimal characters. With the **hmac-sha1-96** option, the key contains 40 hexadecimal characters.

### *Configuring the Encryption Algorithm and Key*

To configure IPSec encryption, include the **encryption** statement and specify an algorithm and key at the [**edit security ipsec security-association** *sa-name* **manual direction (inbound | outbound | bi-directional)**] hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound
    | bi-directional)]
encryption {
    algorithm (des-cbc | 3des-cbc);
    key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 64 bits long.
- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.

**NOTE:** For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409. For 3des-cbc, we recommend that the first 8 bytes not be the same as the second 8 bytes, and that the second 8 bytes be the same as the third 8 bytes.

The key can be one of the following:

- ascii-text—ASCII text key. With the des-cbc option, the key contains 8 ASCII characters. With the 3des-cbc option, the key contains 24 ASCII characters.
- hexadecimal—Hexadecimal key. With the des-cbc option, the key contains 16 hexadecimal characters. With the 3des-cbc option, the key contains 48 hexadecimal characters.

**NOTE:** You cannot configure encryption when you use the AH protocol.

### Configuring Dynamic Security Associations

You configure dynamic SAs with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and do not need to be specified in the configuration. The dynamic SA includes one or more proposals, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

To enable a dynamic SA, follow these steps:

1. Configure IKE proposals and IKE policies associated with these proposals.
2. Configure IPSec proposals and an IPSec policy associated with these proposals.
3. Associate an SA with an IPSec policy.

For more information about IKE policies and proposals, see “Configuring an IKE Policy for Preshared Keys” on page 550 and “Configuring an IKE Proposal (Dynamic SAs Only)” on page 548. For more information about IPSec policies and proposals, see “Configuring the IPSec Policy (ES PIC)” on page 555.

**NOTE:** Dynamic tunnel SAs require an ES PIC.

To configure a dynamic SA, include the dynamic statement at the [edit security ipsec security-association *sa-name*] hierarchy level. Specify an IPSec policy name, and optionally, a 32-packet or 64-packet replay window size.

```
[edit security ipsec security-association sa-name ]
dynamic {
   ipsec-policy policy-name ;
   replay-window-size (32 | 64);
```

```
}
```

**NOTE:** If you want to establish a dynamic SA, the attributes in at least one configured IPSec and IKE proposal must match those of its peer.

The replay window is not used with manual SAs.

## *Configuring an IKE Proposal (Dynamic SAs Only)*

Dynamic SAs require IKE configuration. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway.

You can configure one or more IKE proposals. Each proposal is a list of IKE attributes to protect the IKE connection between the IKE host and its peer.

To configure an IKE proposal and define its properties, include the following statements at the [edit security ike] hierarchy level:

```
[edit security ike]
proposal ike-proposal-name {
    authentication-algorithm (md5 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description ;
    dh-group (group1 | group2);
    encryption-algorithm (3des-cbc | des-cbc | ase-128-cbc | ase-192-cbc | ase-256-cbc);
    lifetime-seconds seconds;
}
```

For information about associating an IKE proposal with an IKE policy, see “Associating Proposals with an IKE Policy” on page 552.

This section discusses the following topics:



### Configuring the Authentication Algorithm for an IKE Proposal

To configure an IKE authentication algorithm, include the authentication-algorithm statement at the [edit security ike proposal *ike-proposal-name*] hierarchy level:

```
[edit security ike proposal ike-proposal-name]
authentication-algorithm (md5 | sha1);
```

The authentication algorithm can be one of the following:

- md5—Produces a 128-bit digest.
- sha1—Produces a 160-bit digest.

### Configuring the Authentication Method for an IKE Proposal

To configure an IKE authentication method, include the authentication-method statement at the [edit security ike proposal *ike-proposal-name*] hierarchy level:

```
[edit security ike proposal ike-proposal-name]
authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
```

The authentication method can be one of the following:

- dsa-signatures—Digital Signature Algorithm (DSA)
- pre-shared-keys—Preshared keys; a key derived from an out-of-band mechanism is used to authenticate an exchange
- rsa-signatures—Public key algorithm that supports encryption and digital signatures

### Configuring the Description for an IKE Proposal

To specify a description for an IKE proposal, include the description statement at the [edit security ike proposal *ike-proposal-name*] hierarchy level:

```
[edit security ike proposal ike-proposal-name]
description description;
```

### Configuring the Diffie-Hellman Group for an IKE Proposal

Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel. It is also used within IKE to establish session keys.

To configure an IKE Diffie-Hellman group, include the dh-group statement at the [edit security ike proposal *ike-proposal-name*] hierarchy level:

```
[edit security ike proposal ike-proposal-name ]
dh-group (group1 | group2);
```

The group can be one of the following:

- group1—Specifies that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- group2—Specifies that IKE use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

group2 provides more security but requires more processing time.

### Configuring the Encryption Algorithm for an IKE Proposal

To configure an IKE encryption algorithm, include the encryption-algorithm statement at the [edit security ike proposal *ike-proposal-name*] hierarchy level:

```
[edit security ike proposal ike-proposal-name ]
encryption-algorithm (3des-cbc | des-cbc);
```

The encryption algorithm can be one of the following:

- 3des-cbc—Encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.
- des-cbc—Encryption algorithm that has a key size of 8 bytes; its key size is 56 bits long.
- aes-128-cbc—Advanced encryption algorithm that has a key size of 16 bytes; its key size is 128 bits long.
- aes-192-cbc—Advanced encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.
- aes-256-cbc—Advanced encryption algorithm that has a key size of 32 bytes; its key size is 256 bits long.

### Configuring the Lifetime for an IKE SA

The IKE lifetime sets the lifetime of an IKE SA. When the IKE SA expires, it is replaced by a new SA (and SPI) or is terminated. The default value IKE lifetime is 3600 seconds.

To configure the IKE lifetime, include the lifetime-seconds statement and specify the number of seconds (180 through 86,400) at the [edit security ike proposal *ike-proposal-name*] hierarchy level:

```
[edit security ike proposal ike-proposal-name ]
lifetime-seconds seconds;
```

### Example: Configuring an IKE Proposal

Configure an IKE proposal:

```
[edit security ike]
proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
}
```

## *Configuring an IKE Policy for Preshared Keys*

An IKE policy defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address, the preshared key for the given peer, and the proposals needed for that connection. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the

negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used. The configured preshared key must also match its peer.

You can create multiple, prioritized proposals at each peer to ensure that at least one proposal will match a remote peer's proposal.

First, you configure one or more IKE proposals; then you associate these proposals with an IKE policy. You can also prioritize a list of proposals used by IKE in the policy statement by listing the proposals you want to use, from first to last.

To configure an IKE policy, include the policy statement at the [edit security ike] hierarchy level and specify a peer address:

```
[edit security ike]
policy ike-peer-address;
```

**NOTE:** The IKE policy peer address must be an IPSec tunnel destination address.

This section discusses the following topics:



### Configuring the Description for an IKE Policy

To specify a description for an IKE policy, include the description statement at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address]
description description;
```

### Configuring the Mode for an IKE Policy

IKE policy has two modes: aggressive and main. By default, main mode is enabled. Main mode uses six messages, in three exchanges, to establish the IKE SA. (These three steps are IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer.) Main mode also allows a peer to hide its identity.

Aggressive mode also establishes an authenticated IKE SA and keys. However, aggressive mode uses half the number of messages, has less negotiation power, and does not provide identity protection. The peer can use the aggressive or main mode to start IKE negotiation; the remote peer accepts the mode sent by the peer.

To configure IKE policy mode, include the mode statement and specify aggressive or main at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address ]
mode (aggressive | main);
```

### Configuring the Preshared Key for an IKE Policy

IKE policy preshared keys authenticate peers. You must manually configure a preshared key, which must match that of its peer. The preshared key can be an ASCII text (alphanumeric) key or a hexadecimal key.

A local certificate is an alternative to the preshared key. Commit will fail if either pre-shared key or local certificate is not configured.

To configure an IKE policy preshared key, include the pre-shared-key statement at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address]
pre-shared-key (ascii-text key | hexadecimal key);
```

### Associating Proposals with an IKE Policy

The IKE policy proposal is a list of one or more proposals associated with an IKE policy.

To configure an IKE policy proposal, include the proposals statement at the [edit security ike policy *ike-peer-address*] hierarchy level and specify one or more proposal names:

```
[edit security ike policy ike-peer-address]
proposals [ proposal-names ];
```

For more information about configuring an individual proposal, see “Configuring an IKE Proposal (Dynamic SAs Only)” on page 548.

### Example: Configuring an IKE Policy

Define two IKE policies: policy 10.1.1.2 and policy 10.1.1.1. Each policy is associated with proposal-1 and proposal-2.

```
[edit security]
ike {
   proposal proposal-1 {
      authentication-method pre-shared-keys;
      dh-group group1;
      authentication-algorithm sha1;
      encryption-algorithm 3des-cbc;
      lifetime-seconds 1000;
   }
   proposal proposal-2 {
      authentication-method pre-shared-keys;
      dh-group group2;
```

```
        authentication-algorithm md5;
        encryption-algorithm des-cbc;
        lifetime-seconds 10000;
    }
    proposal proposal-3 {
        authentication-method rsa-signatures;
        dh-group group2;
        authentication-algorithm md5;
        encryption-algorithm des-cbc;
        lifetime-seconds 10000;
    }
    policy 10.1.1.2 {
        mode main;
        proposals [ proposal-1 proposal-2 ];
        pre-shared-key ascii-text example-pre-shared-key;
    }
    policy 10.1.1.1 {
        local-certificate certificate-filename;
        local-key-pair private-public-key-file;
        mode aggressive;
        proposals [ proposal-2 proposal-3 ]
        pre-shared-key hexadecimal 0102030abbcd;
    }
}
```

**NOTE:** Updates to the current IKE proposal and policy configuration are not applied to the current IKE SA; updates are applied to new IKE SAs.

If you want the new updates to take immediate effect, you must clear the existing IKE security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IKE security association, see the *JUNOS System Basics and Services Command Reference*.

### *Configuring an IPSec Proposal (ES PIC)*

An IPSec proposal lists protocols and algorithms (security services) to be negotiated with the remote IPSec peer.

To configure an IPSec proposal and define its properties, include the following statements at the [edit security ipsec] hierarchy level:

```
[edit security ipsec]
proposal ipsec-proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description description ;
    encryption-algorithm (3des-cbc | des-cbc);
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
}
```

This section discusses the following topics:



### Configuring the Authentication Algorithm for an IPSec Proposal

To configure an IPSec authentication algorithm, include the authentication-algorithm statement at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name]
authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
```

The authentication algorithm can be one of the following:

- hmac-md5-96—Hash algorithm that authenticates packet data. It produces a 128-bit digest. Only 96 bits are used for authentication.
- hmac-sha1-96—Hash algorithm that authenticates packet data. It produces a 160-bit digest. Only 96 bits are used for authentication.

### Configuring the Description for an IPSec Proposal

To specify a description for an IPSec proposal, include the description statement at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level:

```
[edit security ike policy ipsec-proposal-name]
description description;
```

### Configuring the Encryption Algorithm for an IPSec Proposal

To configure the IPSec encryption algorithm, include the encryption-algorithm statement at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name]
encryption-algorithm (3des-cbc | des-cbc);
```

The encryption algorithm can be one of the following:

- 3des-cbc—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- des-cbc—Encryption algorithm that has a block size of 8 bytes; its key size is
- 48 bits long.

**NOTE:** We recommend that you use the triple DES cipher block chaining (3DES-CBC) encryption algorithm.

### Configuring the Lifetime for an IPSec SA

The IPSec lifetime option sets the lifetime of an IPSec SA. When the IPSec SA expires, it is replaced by a new SA (and SPI) or is terminated. A new SA has new authentication and encryption keys, and SPI; however, the algorithms may remain the same if the proposal is not changed. If you do not configure a lifetime and a lifetime is not sent by a responder, the lifetime is 28,800 seconds.

To configure the IPSec lifetime, include the lifetime-seconds statement and specify the number of seconds (180 through 86,400) at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name]
lifetime-seconds seconds;
```

**NOTE:** When a dynamic SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPSec key management system that that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires. When you specify the lifetime, you specify a hard lifetime.

### Configuring the Protocol for a Dynamic IPSec SA

The protocol statement sets the protocol for a dynamic SA. The ESP protocol can support authentication, encryption, or both. The AH protocol is used for strong authentication. AH also authenticates the IP packet. The bundle option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

To configure the protocol for a dynamic SA, include the protocol statement at the [edit security ipsec proposal *ipsec-proposal-name*] hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name ] protocol (ah | esp | bundle);
```

## *Configuring the IPSec Policy (ES PIC)*

An IPSec policy defines a combination of security parameters (IPSec proposals) used during IPSec negotiation. It defines Perfect Forward Secrecy (PFS) and the proposals needed for the connection. During the IPSec negotiation, IPSec looks for an IPSec proposal that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used.

You can create multiple, prioritized IPSec proposals at each peer to ensure that at least one proposal will match a remote peer's proposal.

First, you configure one or more IPSec proposals; then you associate these proposals with an IPSec policy. You can prioritize the proposals in the list by listing them in the order in which the IPSec policy uses them (first to last).

To configure an IPSec policy, include the policy statement at the [edit security ipsec] hierarchy level, specifying the policy name and one or more proposals you want to associate with this policy:

```
[edit security ipsec]
policy ipsec-policy-name {
   proposals [ proposal-names ];
}
```

This section discusses the following topics related to configuring an IPSec policy:



### Configuring Perfect Forward Secrecy

PFS provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys. This statement is optional.

To configure PFS, include the perfect-forward-secrecy statement and specify a Diffie-Hellman group at the [edit security ipsec policy *ipsec-policy-name*] hierarchy level:

```
[edit security ipsec policy ipsec-policy-name]
perfect-forward-secrecy {
   keys (group1 | group2);
}
```

The key can be one of the following:

- group1—Specifies that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- group2—Specifies that IKE use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

group2 provides more security than group1, but requires more processing time.

### Example: IPSec Policy Configuration

Define an IPSec policy, dynamic policy-1, that is associated with two proposals (dynamic-1 and dynamic-2):

```
[edit security ipsec]
proposal dynamic-1 {
   protocol esp;
   authentication-algorithm hmac-md5-96;
   encryption-algorithm 3des-cbc;
   lifetime-seconds 6000;
```

```
}
proposal dynamic-2 {
   protocol esp;
   authentication-algorithm hmac-sha1-96;
   encryption-algorithm 3des-cbc;
   lifetime-seconds 6000;
}
policy dynamic-policy-1 {
   perfect-forward-secrecy {
      keys group1;
   }
   proposals [ dynamic-1 dynamic-2 ];
}
security-association dynamic-sa1 {
   dynamic {
      replay-window-size 64;
      ipsec-policy dynamic-policy-1;
   }
}
```

**NOTE:** Updates to the current IPSec proposal and policy configuration are not applied to the current IPSec SA; updates are applied to new IPSec SAs.

If you want the new updates to take immediate effect, you must clear the existing IPSec security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IPSec security association, see the *JUNOS System Basics and Services Command Reference*.

## Using Digital Certificates (ES PIC)

The statements for configuring digital certificates differ for the AS and MultiServices PICs and the ES PIC. For more information about how to configure digital certificates for adaptive services interfaces, see "Configuring Digital Certificates for Adaptive Services Interfaces" on page 573.

To define the digital certificate configuration for an encryption service interface, include the following statements at the [edit security certificates] and [edit security ike] hierarchy levels:

```
[edit security]
certificates {
   cache-size bytes;
   cache-timeout-negative seconds;
   certification-authority ca-profile-name {
      ca-name ca-identity;
      crl filename;
      encoding (binary | pem);
      enrollment-url url-name;
      file certificate-filename;
      ldap-url url-name;
   }
```

```
    enrollment-retry attempts ;
    local certificate-filename {
      certificate-key-string;
      load-key-file key-file-name;
    }
    maximum-certificates number;
    path-length certificate-path-length;
  }
  ike {
    policy ike-peer-address {
      description policy;
      encoding (binary | pem);
      identity identity-name;
      local-certificate certificate-filename;
      local-key-pair private-public-key-file;
      mode (aggressive | main);
      pre-shared-key (ascii-text key | hexadecimal key);
      proposals [ proposal-names ];
    }
  }
```

For information about how to configure the description and mode statements, see "Configuring the Description for an IKE Policy" on page 551 and "Configuring the Mode for an IKE Policy" on page 551. For information about how to configure the IKE proposal, see "Associating Proposals with an IKE Policy" on page 552

**NOTE:** For digital certificates, the JUNOS software supports only VeriSign CAs for the ES PIC.

To use digital certificates for dynamic SAs, perform the tasks described in the following sections:

- Digital Certificates Overview on page 558
- Obtaining a Certificate from a Certificate Authority (ES PIC) on page 559
- Configuring Digital Certificates (ES PIC) on page 561
- Configuring an IKE Policy for Digital Certificates (ES PIC) on page 565
- Obtaining a Signed Certificate from the CA (ES PIC) on page 566

## *Digital Certificates Overview*

Digital certificates provide a way of authenticating users through a trusted third party called a certificate authority (CA). The CA validates the identity of a certificate holder and "signs" the certificate to attest that it has not been forged or altered.

A certificate includes the following information:

- The distinguished name (DN) of the owner. A DN is a unique identifier and consists of a fully qualified name including not only the common name (CN) of the owner, the owner's organization, and other distinguishing information.
- The public key of the owner.

- The date on which the certificate was issued.
- The date on which the certificate expires.
- The distinguished name of the issuing CA.
- The digital signature of the issuing CA.

The additional information in a certificate allows recipients to decide whether to accept the certificate. The recipient can determine if the certificate is still valid based on the expiration date. The recipient can check whether the CA is trusted by the site based on the issuing CA.

With a certificate, a CA takes the owner's public key, signs that public key with the its own private key, and returns this to the owner as a certificate. The recipient can extract the certificate (containing the CA's signature) with the owner's public key. By using the CA's public key and the CA's signature on the extracted certificate, the recipient can validate the CA's signature and owner of the certificate.

When you use digital certificates, your first send in a request to obtain a certificate from your CA. You then configure digital certificates and a digital certificate IKE policy. Finally, you obtain a digitally signed certificate from a CA.

**NOTE:** Certificates without an alternate subject name are not appropriate for IPSec services.

## *Obtaining a Certificate from a Certificate Authority (ES PIC)*

Certificate authorities manage certificate requests and issue certificates to participating IPSec network devices. When you create a certificate request, you need to provide the information about the owner of the certificate. The required information and its format vary across certificate authorities.

Certificates use names in the X.500 format, a directory access protocol that provides both read and update access. The entire name is called a DN (distinguished name). It consists of a set of components, which often includes a CN (common name), an organization (O), an organization unit (OU), a country (C), a locality (L), and so on.

**NOTE:** For the dynamic registration of digital certificates, the JUNOS software supports only the Simple Certificate Enrollment Protocol (SCEP).

This section contains the following topics:


- Requesting a CA Digital Certificate on page 559
- Generating a Private and Public Key on page 560


### Requesting a CA Digital Certificate

For an encryption interface on an M-series or T-series routing platform, issue the following command to obtain a public key certificate from a CA. The results are saved

in the specified file in the /var/etc/ikecert directory. The CA public key verifies certificates from remote peers.

user@host> **request security certificate enroll filename *filename* ca-name *ca-name* parameters *parameters***

***Example: Requesting a CA Digital Certificate***

Specify a URL to the SCEP server and the name of the certification authority whose certificate you want: mycompany.com. filename 1 is name of the file that stores the result. The output, "Received CA certificate:" provides the signature for the certificate, which allows you to verify (offline) that the certificate is genuine.

```
user@host> request security certificate enroll filename ca_verisign ca-file verisign
   ca-name xyzcompany url
http://pilotonsiteipsec.verisign.com/cgi-bin/pkiclient.exe
URL: http://pilotonsiteipsec.verisign.com/cgi-bin/pkiclient.exe CA name: juniper.net
   CA file: verisign Encoding: binary
Certificate enrollment has started. To see the certificate enrollment status, check the
   key management process (kmd) log file at /var/log/kmd. <----------
```

**NOTE:** Each router is initially manually enrolled with a certificate authority.

## Generating a Private and Public Key

To generate a private and public key, issue the following command:

user@host> **request security key-pair *name* size *key-size* type ( rsa | dsa )**

*name* specifies the filename in which to store the public and private keys.

*key-size* can be 512, 1024, 1596, or 2048 bytes. The default key size is 1024 bytes.

type can be rsa or dsa. The default is RSA.

**NOTE:** When you use SCEP, the JUNOS software only supports RSA.

***Example: Generating a Key Pair***

Generate a private and public key:

```
user@host> request security key-pair batt
Generated key pair, key size 1024, file batt Algorithm RSA
```

## *Configuring Digital Certificates (ES PIC)*

This section includes the following topics:



For information about the minimum digital certificate configuration for IKE, see "Minimum Digital Certificates Configuration for IKE (ES PIC)" on page 540.

### Configuring the Certificate Authority Properties

A CA is a trusted third-party organization that creates, enrolls, validates, and revokes digital certificates.

To configure a certificate authority and its properties for an ES PIC, include the following statements at the [edit security certificates] hierarchy level:

```
[edit security certificates]
certification-authority ca-profile-name {
    ca-name ca-identity;
    crl filename;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
}
```

*ca-profile-name* is the CA profile name.

This section discusses the following topics:



#### *Specifying the Certificate Authority Name*

If you are enrolling with a CA using simple certificate enrollment protocols (SCEP), you need to specify the CA name (CA identity) that is used in the certificate request, in addition to the URL for the SCEP server.

To specify the name of the CA identity, include the ca-name statement at the [edit security certificates certification-authority *ca-profile-name*] hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
ca-name ca-identity;
```

*ca-identity* specifies the CA identity to use in the certificate request. It is typically the CA domain name.

#### *Configuring the Certificate Revocation List*

A certificate revocation list (CRL) contains a list of digital certificates that have been canceled before their expiration date. When a participating peer uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL.

To configure the CA certificate revocation list, include the crl statement and specify the file from which to read the CRL at the [edit security certificates certification-authority *ca-profile-name*] hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
crl filename;
```

#### *Configuring the Type of Encoding Your CA Supports*

By default, encoding is set to binary. Encoding specifies the file format used for the local-certificate and local-key-pair statements. By default, the binary (distinguished encoding rules) format is enabled. Privacy-enhanced mail (PEM) is an ASCII base 64 encoded format. Check with your CA to determine which file formats it supports.

To configure the file format that your CA supports, include the encoding statement and specify a binary or PEM format at the [edit security certificates certification-authority *ca-profile-name*] hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
encoding (binary | pem);
```

#### *Specifying an Enrollment URL*

You specify the CA location where your router should send SCEP-based certificate enrollment requests. To specify the CA location by naming the CA URL, include the enrollment-url statement at the [edit security certificates certification-authority *ca-profile-name*] hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
enrollment-url url-name;
```

*url-name* is the CA location. The format is http://*CA_name*, where *CA_name* is the CA host DNS name or IP address.

#### *Specifying a File to Read the Digital Certificate*

To specify the file from which to read the digital certificate, include the file statement and specify the certificate filename at the [edit security certificates certification-authority *ca-profile-name*] hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
file certificate-filename;
```

#### *Specifying an LDAP URL*

If your CA stores its current CRL at its Lightweight Directory Access Protocol (LDAP) server, you can optionally check your CA CRL list before using a digital certificate. If the digital certificate appears on the CA CRL, your router cannot use it. To access your CA CRL, include the ldap-url statement at the [edit security certificates certification-authority *ca-profile-name*] hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
ldap-url url-name;
```

*url-name* is the certification authority LDAP server name. The format is ldap://*server-name,* where *server-name* is the CA host DNS name or IP address.

### Configuring the Cache Size

By default, the cache size is 2 megabytes (MB). To configure total cache size for digital certificates, include the cache-size statement at the [edit security certificates] hierarchy level:

```
[edit security certificates]
cache-size bytes;
```

*bytes* is the cache size for digital certificates. The range can be from 64 through 4,294,967,295 bytes.

**NOTE:** We recommend that you limit your cache size to 4 MB.

### Configuring the Negative Cache

Negative caching stores negative results and reduces the response time for negative answers. It also reduces the number of messages that are sent to the remote server. Maintaining a negative cache state allows the system to quickly return a failure condition when a lookup attempt is retried. Without a negative cache state, a retry would require waiting for the remote server to fail to respond, even though the system already " knows" that remote server is not responding.

By default, the negative cache is 20 seconds. To configure the negative cache, include the cache-timeout-negative statement at the [edit security certificates] hierarchy level:

```
[edit security certificates]
cache-timeout-negative seconds;
```

*seconds* is the amount of time for which a failed CA or router certificate is present in the negative cache. While searching for certificates with a matching CA identity (domain name for certificates or CA domain name and serial for CRLs), the negative cache is searched first. If an entry is found in the negative cache, the search fails immediately.

**NOTE:** Configuring a large negative cache value can make you susceptible to a denial-of-service (DoS) attack.

### Configuring the Number of Enrollment Retries

By default, the number of enrollment retries is set to 0, an infinite number of retries. To specify how many times a router will resend a certificate request, include the enrollment-retry statement at the [edit security certificates] hierarchy level:

```
[edit security certificates]
enrollment-retry attempts;
```

*attempts* is the number of enrollment retries (0 through 100).

### Configuring the Maximum Number of Peer Certificates

By default, the maximum number of peer certificates to be cached is 1024. To configure the maximum number of peer certificates to be cached, include the maximum-certificates statement at the [edit security certificates] hierarchy statement level:

```
[edit security certificates]
maximum-certificates number;
```

*number* is the maximum number of peer certificates to be cached. The range is from 64 through 4,294,967,295 peer certificates.

### Configuring the Path Length for the Certificate Hierarchy

Certification authorities can issue certificates to other CAs. This creates a tree-like certification hierarchy. The highest trusted CA in the hierarchy is called the *trust anchor*. Sometimes the trust anchor is the root CA, which is usually signed by itself. In the hierarchy, every certificate is signed by the CA immediately above it. An exception is the root CA certificate, which is usually signed by the root CA itself. In general, a chain of multiple certificates may be needed, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs. Such chains, called certification paths, are required because a public key user is only initialized with a limited number of assured CA public keys.

Path length refers to a path of certificates from one certificate to another certificate, based on the relationship of a CA and its "children." When you configure the path length statement, you specify the maximum depth of the hierarchy to validate a certificate from the trusted root CA certificate to the certificate in question. For more

information about the certificate hierarchy, see RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

By default, the maximum certificate path length is set to 15. The root anchor is 1.

To configure path length, include the path-length statement at the [edit security certificates] hierarchy level:

```
[edit security certificates]
path-length certificate-path-length;
```

*certificate-path-length* is the maximum number certificates for the certificate path length. The range is from 2 through 15 certificates.

## Configuring an IKE Policy for Digital Certificates (ES PIC)

An IKE policy for digital certificates defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address and the proposals needed for that connection. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

To configure an IKE policy for digital certificates for an ES PIC, include the following statements at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike]
policy ike-peer-address{
    encoding (binary | pem);
    identity identity-name;
    local-certificate certificate-filename;
    local-key-pair private-public-key-file;
}
```

This section contains the following topics:



### Configuring the Type of Encoding Your CA Supports

By default, the encoding is set to binary. Encoding specifies the file format used for the local-certificate and local-key-pair statements. By default, the binary (distinguished encoding rules) format is enabled. PEM is an ASCII base 64 encoded format. Check with your CA to determine which file formats it supports.

To configure the file format that your CA supports, include the encoding statement and specify a binary or PEM format at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address ]
encoding (binary | pem);
```

### Configuring the Identity to Define the Remote Certificate Name

To define the remote certificate name, include the identity statement at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address]
identity identity-name;
```

*identity-name* defines the identity of the remote certificate name if the identity cannot be learned through IKE (ID payload or IP address).

### Specifying the Certificate Filename

To configure the certificate filename from which to read the local certificate, include the local-certificate statement at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address]
local-certificate certificate-filename;
```

*certificate-filename* specifies the file from which to read the local certificate.

### Specifying the Private and Public Key File

To specify the filename from which to read the public and private key, include the local key-pair statement at the [edit security ike policy *ike-peer-address*] hierarchy level:

```
[edit security ike policy ike-peer-address ]
local-key-pair private-public-key-file;
```

*private-public-key-file* specifies the file from which to read the pair key.

## *Obtaining a Signed Certificate from the CA (ES PIC)*

To obtain signed certificate from the CA, issue the following command:

```
user@host> request security certificate enroll filename filename subject c=us,o=x
   alternative-subject certificate-ip-address certification-authority certificate-authority
   key-file key-file-name domain-name domain-name
```

The results are saved in a specified file to the /var/etc/ikecert directory.

### Example: Obtaining a Signed Certificate

Obtain a CA signed certificate by referencing the configured certification-authority statement local . This statement is referenced by the request security certificate enroll filename m subject c=us,0=x alternative subject 1.1.1.1 certification-authority command.

```
[edit]
security {
   certificates {
      certification-authority local {
         ca-name xyz.company.com;
```

```
            file l;
            enrollment-url "http://www.xyzcompany.com";
        }
    }
}
```

To obtain a signed certificate from the CA, issue the following command:

```
user@host> request security certificate enroll filename l subject c=uk,o=london
    alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv
    domain-name host.xyzcompany.com
CA name: xyz.company.com CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.juniper.net
alternative subject: 10.50.1.4
Encoding: binary
Certificate enrollment has started. To see the certificate enrollment status, check the
    key management process (kmd) log file at /var/log/kmd. <————
```

For information about how to use the operational mode commands to obtain a signed certificate, see the *JUNOS System Basics and Services Command Reference*.

Another way to obtain a signed certificate from the CA is to reference the configured statements such as the URL, CA name, and CA certificate file by means of the certification-authority statement:

```
user@host> request security certificate enroll filename m subject c=us,o=x
    alternative-subject 1.1.1.1 certification-authority local key-file y domain-name
    abc.company.com
```

## Configuring the ES PIC

Configuring the ES PIC associates the configured SA with a logical interface. This configuration defines the tunnel itself (logical subunit, tunnel addresses, maximum transmission unit [MTU], optional interface addresses, and the name of the SA to apply to traffic).

The addresses configured as the tunnel source and destination are the addresses in the outer IP header of the tunnel.

**NOTE:** The tunnel source address must be configured locally on the router, and the tunnel destination address must be a valid address for the security gateway terminating the tunnel.

The M5, M10, M20, and M40 routers support the ES PIC.

You can also configure IPSec on the AS PIC and MultiServices PICs. For information about how to configure IPSec on the AS PIC or MultiServices PIC, see the *JUNOS Services Interfaces Configuration Guide*.

The SA must be a valid tunnel-mode SA. The interface address and destination address listed are optional. The destination address allows the user to configure a static route to encrypt traffic. If a static route uses that destination address as the next hop, traffic is forwarded through the portion of the tunnel in which encryption occurs. For more information about the ES PIC, see the *JUNOS Services Interfaces Configuration Guide*.

### *Example: Configuring the ES PIC*

Configure an IPSec tunnel as a logical interface on the ES PIC. The logical interface specifies the tunnel through which the encrypted traffic travels. The ipsec-sa statement associates the security profile with the interface.

```
[edit interfaces]
es-0/0/0 {
   unit 0 {
      tunnel {
         source tunnel 10.5.5.5; # tunnel source address
         destination 10.6.6.6; # tunnel destination address
      }
      family inet {
         ipsec-sa ipsec-sa; # name of security association to apply to packet
         address 10.1.1.8/32 { # local interface address inside local VPN
         destination 10.2.2.254; # destination address inside remote VPN
      }
   }
}
```

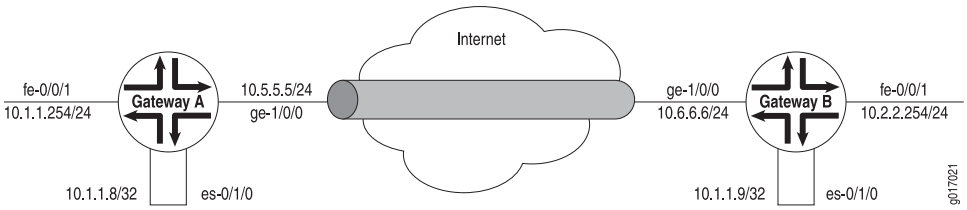
## Configuring Traffic

Traffic configuration defines the traffic that must flow through the tunnel. You configure outbound and inbound firewall filters, which identify and direct traffic to be encrypted and confirm that decrypted traffic parameters match those defined for the given tunnel. The outbound filter is applied to the LAN or WAN interface for the incoming traffic you want to encrypt off of that LAN or WAN. The inbound filter is applied to the ES PIC to check the policy for traffic coming in from the remote host. Because of the complexity of configuring a router to forward packets, no automatic checking is done to ensure that the configuration is correct. Make sure that you configure the router very carefully.

**NOTE:** The valid firewall filters statements for IPSec are destination-port, source-port, protocol, destination-address, and source-address.

In Figure 9 on page 569, Gateway A protects the network 10.1.1.0/24, and Gateway B protects the network 10.2.2.0/24. The gateways are connected by an IPSec tunnel. For more information about firewalls, see the *JUNOS Policy Framework Configuration Guide*.

**Figure 9: Example: IPSec Tunnel Connecting Security Gateways**




The SA and ES interface for security Gateway A are configured as follows:

```
[edit security ipsec]
security-association manual-sa1 {
   manual {
      direction bidirectional {
         protocol esp;
         spi 2312;
         authentication {
            algorithm hmac-md5-96;
            key ascii-text 1234123412341234;
         }
         encryption {
            algorithm 3des-cbc;
            key ascii-text 123456789009876543211234;
         }
      }
   }
}
[edit interfaces es-0/1/0]
unit 0 {
   tunnel {
      source 10.5.5.5;
      destination 10.6.6.6;
   }
   family inet {
      ipsec-sa manual-sa1;
      address 10.1.1.8/32 {
         destination 10.1.1.9;
      }
   }
}
```

The SA and ES interface for security Gateway B are configured as follows:

```
[edit security ipsec]
security-association manual-sa1 {
   manual {
      direction bidirectional {
         protocol esp;
         spi 2312;
         authentication {
            algorithm hmac-md5-96;
            key ascii-text 1234123412341234;
         }
         encryption {
```

```
            algorithm 3des-cbc;
            key ascii-text 1234567890098765432112345;
        }
    }
  }
}
[edit interfaces es-0/1/0]
unit 0 {
  tunnel {
    source 10.6.6.6;
    destination 10.5.5.5;
  }
  family inet {
    ipsec-sa manual-sa1;
    address 10.1.1.9/32; {
      destination 10.1.1.8;
    }
  }
}
```

For a discussion of the filters applied to traffic through the security gateways, see "Example: Configuring an Outbound Traffic Filter" on page 570.

For sample traffic-filter configurations, see the following sections:

- Example: Configuring an Outbound Traffic Filter on page 570
- Example: Applying an Outbound Traffic Filter on page 571
- Example: Configuring an Inbound Traffic Filter for Policy Check on page 571
- Example: Applying an Inbound Traffic Filter to ES PIC for Policy Check on page 572

### *Example: Configuring an Outbound Traffic Filter*

Firewall filters for outbound traffic direct the traffic through the desired IPSec tunnel and ensure that the tunneled traffic goes out the appropriate interface (see Figure 9 on page 569). Here, an outbound firewall filter is created on security Gateway A; it identifies the traffic to be encrypted and adds it to the input side of the interface that carries the internal VPN traffic:

```
[edit firewall]
filter ipsec-encrypt-policy-filter {
  term term1 {
    from {
      source-address { # local network
      10.1.1.0/24;
    }
    destination-address { # remote network
    10.2.2.0/24;
  }
}
then ipsec-sa manual-sa1; # apply SA name to packet
term default {
  then accept;
}
```

**NOTE:** The source address, port, and protocol on the outbound traffic filter must match the destination address, port, and protocol on the inbound traffic filter. The destination address, port, and protocol on the outbound traffic filter must match the source address, port, and protocol on the inbound traffic filter.

### *Example: Applying an Outbound Traffic Filter*

After you have configured the outbound firewall filter, you apply it:

```
[edit interfaces]
fe-0/0/1 {
   unit 0 {
      family inet {
         filter {
            input ipsec-encrypt-policy-filter;
         }
         address 10.1.1.254/24;
      }
   }
}
```

The outbound filter is applied on the Fast Ethernet interface at the [edit interfaces fe-0/0/1 unit 0 family inet] hierarchy level. Any packet matching the IPSec action term (term 1) on the input filter (ipsec-encrypt-policy-filter), configured on the Fast Ethernet interface, is directed to the ES PIC interface at the [edit interfaces es-0/1/0 unit 0 family inet] hierarchy level. If a packet arrives from the source address 10.1.1.0/24 and goes to the destination address 10.2.2.0/24, the Packet Forwarding Engine directs the packet to the ES PIC interface, which is configured with the manual-sa1 SA. The ES PIC receives the packet, applies the manual-sa1 SA, and sends the packet through the tunnel.

The router must have a route to the tunnel endpoint; add a static route if necessary.

### *Example: Configuring an Inbound Traffic Filter for Policy Check*

Here, an inbound firewall filter, which performs the final IPSec policy check, is created on security Gateway A. This check ensures that only packets that match the traffic configured for this tunnel are accepted.

```
filter ipsec-decrypt-policy-filter {
   term term1 { # perform policy check
   from {
      source-address { # remote network
      10.2.2.0/24;
   }
   destination-address { # local network
   10.1.1.0/24;
}
then accept;
```

### *Example: Applying an Inbound Traffic Filter to ES PIC for Policy Check*

After you create the inbound firewall filter, apply it to the ES PIC. Here, the inbound firewall filter (ipsec-decrypt-policy-filter) is applied on the decrypted packet to perform the final policy check. The IPSec manual-sa1 SA is referenced at the [edit interfaces es-1/2/0 unit 0 family inet] hierarchy level and decrypts the incoming packet.

```
[edit interfaces]
es-1/2/0 {
   unit 0 {
      tunnel {
         source 10.5.5.5; # tunnel source address
         destination 10.6.6.6; # tunnel destination address
      }
      family inet {
         filter {
            input ipsec-decrypt-policy-filter;
         }
      ipsec-sa manual-sa1; # SA name applied to packet
         address 10.1.1.8/32 { # local interface address inside local VPN
            destination 10.2.2.254; # destination address inside remote VPN
         }
   }
}
```

The Packet Forwarding Engine directs IPSec packets to the ES PIC. It uses the packet's SPI, protocol, and destination address to look up the SA configured on one of the ES interfaces. The IPSec manual-sa1 SA is referenced at the [edit interfaces es-1/2/0 unit 0 family inet] hierarchy level and is used to decrypt the incoming packet. When the packets are processed (decrypted, authenticated, or both), the input firewall filter (ipsec-decrypt-policy-filter) is applied on the decrypted packet to perform the final policy check. Term1 defines the decrypted (and verified) traffic and performs the required policy check.

**NOTE:** The inbound traffic filter is applied after the ES PIC has processed the packet, so the decrypted traffic is defined as any traffic that the remote gateway is encrypting and sending to this router. IKE uses this filter to determine the policy required for a tunnel. This policy is used during the negotiation with the remote gateway to find the matching SA configuration.

## Configuring an ES Tunnel Interface for a Layer 3 VPN

To configure an ES tunnel interface for a Layer 3 VPN, you need to configure an ES tunnel interface on the provider edge (PE) router and on the customer edge (CE) router. You also need to configure IPSec on the PE and CE routers. For more information about configuring an ES tunnel for a Layer 3 VPN, see the *JUNOS VPNs Configuration Guide*.

## Configuring Digital Certificates for Adaptive Services Interfaces

A digital certificate implementation uses the public key infrastructure (PKI), which requires you to generate a key pair consisting of a public key and a private key. The keys are created with a random number generator and are used to encrypt and decrypt data. In networks that do not use digital certificates, an IPSec-enabled device encrypts data with the private key and IPSec peers decrypt the data with the public key.

With digital certificates, the key sharing process requires an additional level of complexity. First, you and your IPSec peers request a certificate authority (CA) to send you a CA certificate that contains the public key of the CA. Next you request the CA to enroll a local digital certificate that contains the public key and some additional information. When the CA processes your request, it signs your local certificate with the private key of the CA. Then you install the CA certificate and the local certificate in your routing platform and load the CA in the remote devices before you can establish IPSec tunnels with your peers.

**NOTE:** For digital certificates, the JUNOS software supports VeriSign, Entrust, Cisco Systems, and Microsoft Windows CAs for the AS and MultiServices PICs.

To define digital certificates configuration for J-series Services Routers and Adaptive Services (AS) and MultiServices PICs installed on M-series and T-series routing platforms, include the following statements at the [edit security pki] hierarchy level:

```
[edit security]
pki {
    ca-profile ca-profile-name {
        ca-identity ca-identity;
        enrollment {
            url-name;
            retry number-of-enrollment-attempts;
            retry-interval seconds;
        }
        revocation-check {
            disable;
            crl {
                disable on-download-failure;
                refresh-interval number-of-hours;
                url {
                    url-name;
                    password;
                }
            }
        }
    }
}
```

**NOTE:** For more information about how to configure IPSec for an adaptive services interface, see the "IPSec" chapter of the *JUNOS Feature Guide* and the "IPSec Services Configuration Guidelines" chapter of the *JUNOS Services Interfaces Configuration Guide*.

The following steps enable you to implement digital certificates on J-series Services Routers and AS and MultiServices PICs installed on M-series and T-series routing platforms:

- Configuring the Certificate Authority Properties on page 574
- Configuring the Certificate Revocation List on page 575
- Managing Digital Certificates on page 577
- Configuring the Auto-Reenrollment Properties on page 580

## *Configuring the Certificate Authority Properties*

A CA is a trusted third-party organization that creates, enrolls, validates, and revokes digital certificates.

To configure a certificate authority and its properties for the AS and MultiServices PICs, include the following statements at the [edit security pki] hierarchy level:

```
[edit security pki]
ca-profile ca-profile-name {
    ca-identity ca-identity;
    enrollment {
        url url-name;
        retry number-of-attempts;
        retry-interval seconds;
    }
}
```

This section includes the following topics:

- Specifying the CA Profile Name on page 574
- Specifying an Enrollment URL on page 575
- Specifying the Enrollment Properties on page 575

### Specifying the CA Profile Name

The CA profile contains the name and URL of the CA or RA, as well as some retry-timer settings. CA certificates issued by Entrust, VeriSign, Cisco Systems, and Microsoft are compatible with the J-series Services Routers and AS and MultiServices PICs installed in the M-series and T-series routing platforms.

To specify the CA profile name, include the ca-profile statement at the [edit security pki] security level:

```
[edit security pki]
ca-profile ca-profile-name;
```

You also need to specify the name of the CA identity used in the certificate request. This name is typically the domain name. To specify the name of the CA identity, include the ca-identity statement at the [edit security pki ca-profile *ca-profile-name*] level:

```
[edit security pki ca-profile ca-profile-name]
ca-identity ca-identity;
```

### Specifying an Enrollment URL

You specify the CA location where your router should send the SCEP-based certificate enrollment requests. To specify the CA location by naming the CA URL, include the url statement at the [edit security pki enrollment] hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
url url-name;
```

*url-name* is the CA location. The format is http://*CA-name*, where *CA-name* is the CA host DNS name or IP address.

### Specifying the Enrollment Properties

You can specify the number of times a router will resend a certificate request and the amount of time, in seconds, the router should wait between enrollment attempts.

By default, the number of enrollment retries is set to 0, an infinite number of retries. To specify how many times a router will resend a certificate request, include the retry *number-of-attempts* statement at the [edit security pki ca-profile *ca-profile-name* enrollment] hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
retry number-of-attempts;
```

The range for *number-of-attempts* is from 0 through 100.

To specify the amount of time, in seconds that a router should wait between enrollment attempts, include the retry-interval *seconds* statement at the [edit security pki ca-profile *ca-profile-name* enrollment] hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
retry-interval seconds;
```

The range for *seconds* is from 0 through 3600.

## *Configuring the Certificate Revocation List*

A certificate revocation list (CRL) contains a list of digital certificates that have been canceled before their expiration date. When a participating peer uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL.

CRLs issued by Entrust, VeriSign, and Microsoft are compatible with the J-series services Routers and AS and MultiServices PICs installed in the M-series and T-series routing platforms.

**NOTE:** By default, certificate revocation list verification is enabled. You can disable CRL verification by including the disable statement at the [edit security pki ca-profile *ca-profile-name* revocation-check] hierarchy level.

To configure the CA certificate revocation list, include the following statements at the [edit security pki ca-profile *ca-profile-name* revocation-check] hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check]
crl {
    disable on-download-failure;
    refresh-interval number-of-hours;
    url {
        url-name;
        password;
    }
}
```

**NOTE:** If you manually download the CRL, you must install it manually on the routing platform. Issue the operational mode command request security pki crl load ca-profile *ca-profile-name* filename *path/filename*. For more information, see the *JUNOS System Basics and Services Command Reference*.

This section contains the following topics:



### Specifying an LDAP URL

You can specify the URL for the Lightweight Directory Access Protocol (LDAP) server where your CA stores its current CRL. If the CA includes the Certificate Distribution Point (CDP) in the digital certificate, you do not need to specify a URL for the LDAP server. The CDP is a field within the certificate that contains information about how to retrieve the CRL for the certificate. The router uses this information to download the CRL automatically.

Configure an LDAP URL if you want to use a different CDP from the one specified in the certificate. Any LDAP URL you configure takes precedence over the CDP included in the certificate.

You can configure up to three URLs for each CA profile.

If the LDAP server requires a password to access the CRL, you need to include the password statement.

To configure the routing platform to retrieve the CRL from the LDAP server, include the url statement and specify the URL name at the [edit security pki ca-profile *ca-profile-name* revocation-check crl] hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
url {
   url-name;
}
```

*url-name* is the certificate authority LDAP server name. The format is ldap://*server-name*, where *server-name* is the CA host DNS name or IP address.

To specify to use a password to access the CRL, include the password statement at the [edit security pki ca-profile *ca-profile-name* revocation-check crl url] hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl url]
password password;
```

*password* is the secret password that the LDAP server requires for access.

### Configuring the Interval Between CRL Updates

By default, the time interval between CRL updates is 24 hours. To configure the amount of time between CRL updates, include the refresh-interval statement at the [edit security pki ca-profile *ca-profile-name* revocation-check crl] hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
refresh-interval number-of-hours;
```

The range for number of hours is from 0 through 8784.

### Overriding Certificate Verification if CRL Download Fails

By default, if the router either cannot access the LDAP URL or retrieve a valid certificate revocation list, certificate verification fails and the IPSec tunnel is not established. To override this behavior and permit the authentication of the IPSec peer when the CRL is not downloaded, include the disable on-download-failure statement at the [edit security pki ca-profile *ca-profile-name* revocation-check crl] hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
disable on-download-failure;
```

## *Managing Digital Certificates*

After you configure the CA profile, you can request a CA certificate from the trusted CA. Next, you must generate a public/private key pair. When the key pair is available, you can generate a local certificate either online or manually.

This section contains the following topics:

## Requesting a CA Digital Certificate

For J-series Services Routers and AS and MultiServices PICs installed on M-series and T-series routing platforms, issue the following command to obtain a digital certificate from a CA. Specify a configured *ca-profile-name* to request a CA certificate from the trusted CA.

user@host>**request security pki ca-certificate enroll ca-profile *ca-profile-name***

For information about how to configure a CA profile see, "Configuring the Certificate Authority Properties" on page 574.

### *Example: Requesting a CA Digital Certificate*

In this example, the certificate is enrolled online and installed into the routing platform automatically.

user@host> **request security pki ca-certificate enroll ca-profile entrust**

```
Received following certificates:
Certificate: C=us, O=juniper
 Fingerprint:00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
Certificate: C=us, O=juniper, CN=First Officer
 Fingerprint:bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
Certificate: C=us, O=juniper, CN=First Officer
 Fingerprint:46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Do you want to load the above CA certificate ? [yes,no] (no) yes
```

**NOTE:** If you obtain the CA certificate directly from the CA (for example, as an e-mail attachment or Web site download), you can install it with the request security pki ca-certificate load command. For more information, see the *JUNOS System Basics and Services Command Reference*.

## Generating a Public/Private Key Pair

After obtaining a certificate for an AS PIC or MultiServices PIC, you must generate a public-private key before you can generate a local certificate. The public key is included in the local digital certificate and the private key is used to decrypt data received from peers. To generate a public-private key pair, issue the request security pki generate-key-pair certificate-id *certificate-id-name* command.

### *Example: Generating a Key Pair*

Generate a public/private key for an AS PIC or MultiServices PIC:

user@host>**request security pki generate-key-pair certificate-id local-entrust2**
Generated key pair local-entrust2, key size 1024 bits

### Generating and Enrolling a Local Digital Certificate

You can generate and enroll local digital certificates either online or manually. To generate and enroll a local certificate online by using the Simple Certificate Enrollment Protocol (SCEP) for an AS PIC or MultiServices PIC, issue the request security pki local-certificate enroll command. To generate a local certificate request manually in the PKCS-10 format, issue the request security pki generate-certificate-request command.

If you create the local certificate request manually, you must also load the certificate manually. To manually install a certificate in your routing platform, issue the request security pki local-certificate load command.

#### *Example: Generating a Local Certificate Manually*

Generate a local certificate request manually and send it to the CA for processing:

```
user@host> request security pki generate-certificate-request certificate-id
  local-entrust2 domain-name router2.juniper.net filename entrust-req2
subject cn=router2.juniper.net


Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHAxLmp1bmlwZXIubmV0MIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFklQws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8ElwTJlkmIt2cB3yifB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8oOXyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjAOBgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5SOQXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH4O6gQ3G
3iHOZfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteolZCiZ7OfO9Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

The trusted CA digitally signs the local certificate and returns it to you. Copy the certificate file into the routing platform and load the certificate:

```
user@host> request security pki local-certificate load filename /tmp/router2-cert
  certificate-id local-entrust2
Local certificate local-entrust2 loaded successfully
```

**NOTE:** The name of the file sent to you by the CA might not match the name of the certificate identifier. However, the certificate-id name must always match the name of the key pair you generated for the routing platform.

After the local and CA certificates have been loaded, you can reference them in your IPSec configuration. Using default values in the AS and MultiServices PICs, you do not need to configure an IPSec proposal or an IPSec policy. However, you must configure an IKE proposal that specifies the use of digital certificates, reference the

IKE proposal and locate the certificate in an IKE policy, and apply the CA profile to the service set.

For more information about how to configure an IKE proposal for an AS PIC or MultiServices PIC, see the "IPSec Services Configuration Guidelines" chapter in the *JUNOS Services Interfaces Configuration Guide*.

### *Configuring the Auto-Reenrollment Properties*

Use the auto-re-enrollment statement to configure automatic reenrollment of a specified existing router certificate before its existing expiration date. This function automatically reenrolls the router certificate. The reenrollment process requests the certificate authority (CA) to issue a new router certificate with a new expiration date. The date of auto-reenrollment is determined by the following parameters:

- re-enroll-trigger-time—The percentage of the difference between the router certificate start date/time (when the certificate was generated) and the validity period; used to specify how long auto-reenrollment should be initiated before expiration.
- validity-period—The number of days after issuance when the router certificate will expire, as set when a certificate is generated.

**NOTE:** By default, this feature is not enabled unless configured explicitly. This means that a certificate that does not have auto-reenrollment configured will expire on its normal expiration date.

The ca-profile statement specifies which CA will be contacted to reenroll the expiring certificate. This is the CA that issued the original router certificate.

The challenge-password statement provides the issuing CA with the router certificate's password, as set by the administrator and normally obtained from the SCEP enrollment Web page of the CA. The password is 16 characters in length.

Optionally, the router certificate key pair can be regenerated by using the re-generate-keypair statement.

To configure the auto-re-enrollment statement and its properties, include the following statements at the [edit security pki] hierarchy level:

```
[edit security pki]
auto-re-enrollment {
    certificate-id {
        ca-profile ca-profile-name;
        challenge-password password;
        re-enroll-trigger-time percentage;
        re-generate-keypair;
        validity-period days;
    }
}
```

*percentage* is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

*days* is the number of days for the validity period. The range can be from 1 through 4095.

This section contains the following topics:



### Specify the Certificate ID

Use the certificate-id statement to specify the name of the router certificate to configure for auto-reenrollment. To specify the certificate ID, include the statement at the [edit security pki auto-re-enrollment] hierarchy level:

```
[edit security pki auto-re-enrollment]
certificate-id certificate-name;
```

### Specify the CA Profile

Use the ca-profile statement to specify the name of the CA profile from the router certificate previously specified by certificate ID. To specify the CA profile, include the statement at the [edit security pki auto-re-enrollment certificate-id *certificate-name*] hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
ca-profile ca-profile-name;
```

**NOTE:** The referenced ca-profile must have an enrollment URL configured at the [edit security pki ca-profile *ca-profile-name* enrollment url] hierarchy level.

### Specify the Challenge Password

The challenge password is used by the CA specified by the PKI certificate ID for reenrollment and revocation. To specify the challenge password, include the following statement at the [edit security pki auto-re-enrollment certificate-id *certificate-name*] hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
challenge-password password;
```

### Specify the Reenroll Trigger Time

Use the re-enroll-trigger-time statement to set the percentage of the validity period before expiration at which reenrollment occurs. To specify the reenroll trigger time, include the following statement at the [edit security pki auto-re-enrollment certificate-id *certificate-name*] hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
re-enroll-trigger-time percentage;
```

*percentage* is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

### Specify the Regenerate Key Pair

When a regenerate key pair is configured, a new key pair is generated during reenrollment. On successful reenrollment, a new key pair and new certificate replace the old certificate and key pair. To generate a new key pair, include the following statement at the [edit security pki auto-re-enrollment certificate-id *certificate-name*] hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
re-generate-keypair;
```

### Specify the Validity Period

The validity-period statement specifies the router certificate validity period, in number of days, that the specified router certificate remains valid. To specify the validity period, include the statement at the [edit security pki auto-re-enrollment certificate-id *certificate-name*] hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
validity-period days;
```

*days* is the number of days for the validity period. The range can be from 1 through 4095.

## Configuring Trace

To configure trace options, specify flags using the traceoptions statement:

```
[edit security]
traceoptions {
   file filename <files number> <size size>;
   flag all;
   flag database;
   flag general;
   flag ike;
   flag parse;
   flag policy-manager;
   flag routing-socket;
   flag timer;
}
```

You can include these statements at the following hierarchy levels:

- [edit security]
- [edit services ipsec-vpn]

You cannot configure these traceoptions statements at both hierarchy levels. Include the traceoptions statement at the [edit services ipsec-vpn] hierarchy level to trace IPSec events for adaptive services interfaces. For more information, see the "IPSec Services Configuration Guidelines" chapter of the *JUNOS Services Interfaces Configuration Guide*.

Trace option output is recorded in the /var/log/kmd file.

You can specify one or more of the following security tracing flags:

- all—Trace all security events
- database—Trace database events
- general—Trace general events
- ike—Trace IKE module processing
- parse—Trace configuration processing
- policy-manager—Trace policy manager processing
- routing-socket—Trace routing socket messages
- timer—Trace internal timer events

## Authentication Key Update Mechanism

You can configure an authentication key update mechanism for the Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) routing protocols. This mechanism allows you to update authentication keys without interrupting associated routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

To configure this feature, include the authentication-key-chains statement at the [edit security] level, and include the authentication-key-chain statement for the BGP or LDP routing protocols at the [edit protocols] level.

For more information, see the following sections:

- Configuring Authentication Key Updates on page 583
- Configuring BGP and LDP for Authentication Key Updates on page 584

### *Configuring Authentication Key Updates*

To configure the authentication key update mechanism, include the key-chain statement at the [edit security authentication-key-chains] hierarchy level, and specify the key option to create a key-chain consisting of several authentication keys.

[edit security authentication-key-chains]

```
key-chain key-chain-name {
    key key {
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
    }
}
```

key-chain—Assigns a name to the key-chain mechanism. This name is also configured at the [edit protocols bgp] or the [edit protocols ldp] hierarchy levels to associate unique authentication key-chain attributes as specified using the following options:

- key—Each key within a key-chain is identified by a unique integer value. The range is from 0 through 63.
- secret—Each key must specify a secret in encrypted text or plain text format. Even if you enter the secret data in plain-text format, the secret always appears in encrypted format.
- start-time—Start times for authentication key updates are specified in UTC (Coordinated Universal Time), and must be unique within the key-chain.

### *Configuring BGP and LDP for Authentication Key Updates*

To configure the authentication key update mechanism for the BGP and LDP routing protocols, include the authentication-key-chain statement at the [edit protocols (bgp | ldp)] hierarchy level to associate each routing protocol with the [edit security authentication-key-chains] authentication keys.

```
[edit protocols (bgp | ldp)]
group group-name {
    neighbor address {
        authentication-key-chain key-chain-name;
    }
}
```

**NOTE:** Beginning with JUNOS Release 7.6, when configuring the authentication key update mechanism for BGP, you cannot commit the 0.0.0.0/allow statement with authentication keys or key chains. The CLI issues a warning and fails to commit such configurations.

For information about the BGP protocol, see the *JUNOS Routing Protocols Configuration Guide*.

## Configuring SSH Host Keys for Secure Copy

Secure Shell (SSH) uses encryption algorithms to generate a host, server, and session key system that ensures secure data transfer. You can configure SSH host keys to support secure copy (SCP) as an alternative to FTP for the background transfer of data such as configuration archives and event logs. To configure SSH support for SCP, you must complete the following tasks:

- Specify SSH known hosts by including hostnames and host key information in the Routing Engine configuration hierarchy.
- Set an SCP URL to specify the host from which to receive data. Setting this attribute automatically retrieves SSH host key information from the SCP server.
  - Verify that the host key is authentic.
  - Accept the secure connection. Accepting this connection automatically stores host key information in the local host key database. Storing host key information in the configuration hierarchy automates the secure handshake and allows background data transfer using SCP.

This section contains the following topics:



### Configuring SSH Known Hosts

To configure SSH known hosts, include the host statement, and specify hostname and host key options for trusted servers at the [edit security ssh-known-hosts] hierarchy level:

```
[edit security ssh-known-hosts]
host corporate-archive-server, ip-address {
    dsa-key key;
}
host archive-server-url {
    rsa-key key;
}
host server-with-ssh-version-1, ip-address {
    rsa1-key key;
}
```

Host keys are one of the following:

- dsa-key—Base64 encoded Digital Signature Algorithm (DSA) key.
- rsa-key—Base 64 encoded RSA public key algorithm, which supports encryption and digital signatures.
- rsa1-key—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1 and SSH version 2.

### Configuring Support for SCP File Transfer

To configure a known host to support background SCP file transfers, include the archive-sites statement at the [edit system archival configuration] hierarchy level.

```
[edit system archival configuration]
archive-sites {
    scp://username<:password>@host<:port>/url-path;
```

}

**NOTE:** When specifying a URL in a JUNOS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example,
"scp://*username*<:*password*>@[*host*]<:*port*>/*url-path*";

Setting the archive-sites statement to point to an SCP URL triggers automatic host key retrieval. At this point, the JUNOS system software connects to the SCP host to fetch the SSH public key, displays the host key message digest or fingerprint as output to the console, and terminates the connection to the server.

```
user@host# set system archival configuration archive-sites "<scp-url-path>"
The authenticity of host <my-archive-server (<server-ip-address>)> can't be established.
    RSA key fingerprint is <ascii-text key>. Are you sure you want to continue connecting
    (yes/no)?
```

To verify that the host key is authentic, compare this fingerprint with a fingerprint that you obtain from the same host using a trusted source. If the fingerprints are identical, accept the host key by entering yes at the prompt. The host key information is then stored in the Routing Engine configuration and supports background data transfers using SCP.

## *Updating SSH Host Key Information*

Typically, SSH host key information is automatically retrieved when you set a URL attribute for SCP using the archival configuration archive-sites statement at the [edit system] hierarchy level. However, if you need to manually update the host key database, use one of the following methods.

### Retrieving Host Key Information Manually

To manually retrieve SSH public host key information, use the fetch-from-server option with the set security ssh-known-hosts command. You must include a hostname attribute with the set security ssh-known-hosts fetch-from-server command to specify the host from which to retrieve the SSH public key.

```
user@host# set security ssh-known-hosts fetch-from-server <hostname>
```

### Importing Host Key Information from a File

To manually import SSH host key information from the known-hosts file located at /var/tmp/known-hosts on the server, include the load-key-file option with the set security ssh-known-hosts command. You must include the path to the known-hosts file with the set security ssh-known-hosts load-key-file command to specify the location from which to import host key information.

```
user@host# set security ssh-known-hosts load-key-file /var/tmp/known-hosts
```

## Importing SSL Certificates for JUNOScript Support

A JUNOScript client application can use one of four protocols to connect to the JUNOScript server on a router: clear-text (a JUNOScript-specific protocol for sending unencrypted text over a TCP connection), SSH, SSL, or Telnet. For clients to use the SSL protocol, you must copy an X.509 authentication certificate onto the router, as described in this section. (You must also include the xnm-ssl statement at the [edit system services] hierarchy level; for more information, see "Configuring SSL Service for JUNOScript Client Applications" on page 146.)

**NOTE:** The xnm-ssl statement does not apply to standard IPSec services.

For detailed information about configuring SSL for JUNOScript clients, see the *JUNOScript API Guide*.

After obtaining an X.509 authentication certificate and private key, copy it to the router by including the local statement at the [edit security certificates] hierarchy level:

```
[edit security certificates]
local certificate-name {
    load-key-file (filename | url);
}
```

*certificate-name* is a name you choose to identify the certificate uniquely (for example, junoscript-ssl-client-*hostname*, where *hostname* is the computer where the client application runs).

*filename* is the pathname of the file on the local disk that contains the paired certificate and private key (assuming you have already used another method to copy them to the router's local disk).

*url* is the URL to the file that contains a paired certificate and private key (for instance, on the computer where the JUNOScript client application runs).

For more information about specifying URLs and pathnames, see the *JUNOS CLI User Guide*.

**NOTE:** The CLI expects the private key in the *URL-or-path* file to be unencrypted. If the key is encrypted, the CLI prompts you for the passphrase associated with it, decrypts it, and stores the unencrypted version.

The load-key-file statement acts as a directive that copies the contents of the certificate file into the configuration. When you view the configuration, the CLI displays the string of characters that constitute the private key and certificate, marking them as SECRET-DATA. The load-key-file keyword is not recorded in the configuration.

## Configuring Internal IPSec for JUNOS-FIPS

In a JUNOS-FIPS environment, routers with two Routing Engines must use IPSec for internal communication between the Routing Engines. You configure internal IPSec after you install JUNOS-FIPS. You must be a Crypto Officer to configure internal IPSec.

To configure internal IPSec, include the security-association statement at the [edit security] hierarchy level:

```
[edit security]
ipsec {
    internal {
        security-association {
            manual {
                direction (bidirectional | inbound | outbound) {
                    protocol esp;
                    spi spi-value;
                    encryption {
                        algorithm 3des-cbc;
                        key ascii-text ascii-text-string;
                    }
                }
            }
        }
    }
}
```

This section describes the following tasks for configuring internal IPSec:



### *Configuring the SA Direction*

To configure the IPSec SA direction, include the direction statement at the [edit security ipsec internal security-association manual] hierarchy level:

```
direction (bidirectional | inbound | outbound);
```

The value can be one of the following:

- bidirectional—Apply the same SA values in both directions between Routing Engines.
- inbound—Apply these SA properties only to the inbound IPSec tunnel.
- outbound—Apply these SA properties only to the outbound IPSec tunnel.

If you do not configure the SA to be bidirectional, you must configure SA parameters for IPSec tunnels in both directions. The following example uses an inbound and outbound IPSec tunnel:

```
[edit security]
ipsec {
   internal {
      security-association {
         manual {
            direction inbound {
               protocol esp;
               spi 512;
               encryption {
                  algorithm 3des-cbc;
                  key ascii-text “$.KL3rnglH7,theOPcn87lxfpe9GJKdme”;
               }
            }
            direction outbound {
               protocol esp;
               spi 513;
               encryption {
                  algorithm 3des-cbc;
                  key ascii-text “.n87lnglH7,thxefpe9GJKdme.KL3rOPc”;
               }
            }
         }
      }
   }
}
```

### *Configuring the IPSec SPI*

A security parameter index (SPI) is a 32-bit index identifying a security context between a pair of Routing Engines. To configure the IPSec Security Parameter Index (SPI) value, include the spi statement at the [edit security ipsec internal security-association manual direction] hierarchy level:

```
spi value;
```

The value must be from 256 through 16639.

### *Configuring the IPSec Key*

To configure the ASCII text key, include the key statement at the [edit security ipsec internal security-association manual direction encryption] hierarchy level:

```
key ascii-text ascii-text-string;
```

The value must be from 256 through 16639. You must enter the key ASCII value twice and the strings entered must match, or the key will not be set. The ASCII text key is never displayed in plain text.

### *Example: Configuring Internal IPSec*

Configure a bidirectional IPSec SA with an SPI value of 512 and a key value conforming to the FIPS 140-2 rules:

```
[edit security]
ipsec {
   internal {
      security-association {
         manual {
            direction bidirectional {
               protocol esp;
               spi 512;
               encryption {
                  algorithm 3des-cbc;
                  key ascii-text “$9$90j.COIek8X7VevbYgoji1rh”;
               }
            }
         }
      }
   }
}
```

Chapter 17

# Summary of Security Services Configuration Statements

The following sections explain each of the security services configuration statements. The statements are organized alphabetically.

## algorithm

**Syntax** algorithm 3des-cbc;

**Hierarchy Level** [edit security ipsec internal security-association manual direction encryption]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Select the encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPSec security association (SA) configuration.

**Options** Only 3des-cbc is supported.

**Usage Guidelines** See "Configuring Internal IPSec for JUNOS-FIPS" on page 588.

**Required Privilege Level** Crypto Officer—To add and view this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## authentication

**Syntax**

```
authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
}
```

**Hierarchy Level** [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure IP Security (IPSec) authentication parameters for manual security association (SA).

**Options** algorithm—Hash algorithm that authenticates packet data. It can be one of the following:

- hmac-md5-96—Produces a 128-bit digest.
- hmac-sha1-96—Produces a 160-bit digest.

key—Type of authentication key. It can be one of the following:

- ascii-text key—ASCII text key. For hmac-md5-96, the key is 16 ASCII characters; for hmac-sha1-96, the key is 20 ASCII characters.
- hexadecimal key—Hexadecimal key. For hmac-md5-96, the key is 32 hexadecimal characters; for hmac-sha1-96, the key is 40 hexadecimal characters.

**Usage Guidelines** See "Configuring the Authentication Algorithm and Key" on page 546.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## authentication-algorithm

See the following sections:

- authentication-algorithm (IKE) on page 593
- authentication-algorithm (IPSec) on page 593

### *authentication-algorithm (IKE)*

**Syntax** authentication-algorithm (md5 | sha1);

**Hierarchy Level** [edit security ike proposal *ike-proposal-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the Internet Key Exchange (IKE) authentication algorithm.

**Options** authentication-algorithm—Hash algorithm that authenticates packet data. It can be one of two algorithms:

- md5—Produces a 128-bit digest.
- sha1—Produces a 160-bit digest.

**Usage Guidelines** See "Configuring the Authentication Algorithm for an IKE Proposal" on page 548.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *authentication-algorithm (IPSec)*

**Syntax** authentication-algorithm (hmac-md5-96 | hmac-sha1-96);

**Hierarchy Level** [edit security ipsec proposal *ipsec-proposal-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the IPSec authentication algorithm.

**Options** authentication-algorithm—Hash algorithm that authenticates packet data. It can be one of two algorithms:

- hmac-md5-96—Produces a 128-bit digest.
- hmac-sha1-96—Produces a 160-bit digest.

**Usage Guidelines** See "Configuring the Authentication Algorithm for an IPSec Proposal" on page 554.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## authentication-key-chains

**Syntax**

```
authentication-key-chains {
    key-chain key-chain-name {
        description text-string;
        key key {
            secret secret-data;
            start-time yyyy-mm-dd.hh:mm:ss;
        }
        tolerance seconds;
    }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in JUNOS Release 7.6.

**Description** Configure authentication key updates for the Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) routing protocols. When an authentication-key-chain statement is configured at the [edit security] hierarchy level, and associated with the BGP and LDP protocols at the [edit protocols] hierarchy level, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF), and Resource Reservation Setup Protocol (RSVP).

**Options**

key-chain—Keychain name. This name is configured at the [edit protocols bgp] or the [edit protocols ldp] hierarchy level to associate unique authentication key-chain attributes with each protocol as specified using the following options:

- description—A text description of the authentication-key-chain. Put the text-string in quotes (“text description”).
- key—Each key within a keychain is identified by a unique integer value.

  **Range:** 0 through 63

  - secret—Each key must specify a secret in encrypted text or plain text format. The secret always appears in encrypted format.
  - start-time—Start times are specified in UTC (Coordinated Universal Time), and must be unique within the keychain.
- tolerance—Specify the clock skew tolerance, in seconds.

  **Range:** 0 through 999999999

**Usage Guidelines** See “Configuring Authentication Key Updates” on page 583.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## authentication-method

**Syntax** authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);

**Hierarchy Level** [edit security ike proposal *ike-proposal-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the IKE authentication method.

**Options** dsa-signatures—Digital Signature Algorithm (DSA)

rsa-signatures—A public key algorithm, which supports encryption and digital signatures

pre-shared-keys—A key derived from an out-of-band mechanism; the key authenticates the exchange

**Usage Guidelines** See "Configuring the Authentication Algorithm and Key" on page 546.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## auto-re-enrollment

**Syntax**

```
auto-re-enrollment {
   certificate-id {
      ca-profile ca-profile-name;
      challenge-password password;
      re-enroll-trigger-time percentage;
      re-generate-keypair;
      validity-period days;
   }
}
```

**Hierarchy Level** [edit security pki]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** Specify auto-reenrollment parameters for a certificate authority (CA) issued router certificate. Auto-reenrollment requests that the issuing CA replace a router certificate before its specified expiration date.

**Options** The remaining statements are explained separately.

**Usage Guidelines** See “Configuring the Auto-Reenrollment Properties” on page 580.

**Required Privilege Level** admin—To view this statement in the configuration.
admin–control—To add this statement to the configuration.

**Related Topics** Configuring Digital Certificates for Adaptive Services Interfaces on page 573

## auxiliary-spi

**Syntax** auxiliary-spi *auxiliary-spi-value*;

**Hierarchy Level** [edit security ipsec security-association *sa-name* manual direction (JUNOS Software) (inbound | outbound | bi-directional)]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the auxiliary Security Parameter Index (SPI) for a manual SA. Use the auxiliary SPI when you configure the protocol statement to use the bundle option.

**Options** *auxiliary-spi-value*—Arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).
**Range:** 256 through 16,639

**Usage Guidelines** See “Configuring the Auxiliary Security Parameter Index” on page 545. For information about SPI, see “Configuring the Security Parameter Index” on page 545 and spi.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ca-identity

**Syntax** ca-identity *ca-identity*;

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name*]

**Release Information** Statement introduced in JUNOS Release 7.5.

**Description** Specify the certificate authority (CA) identity to use in requesting digital certificates for J-series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M-series and T-series routing platforms.

**Options** *ca-identity*—The name of the CA identity. This name is typically the domain name of the CA.

**Usage Guidelines** See "Specifying the CA Profile Name" on page 574.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ca-name

**Syntax** ca-name *ca-identity*;

**Hierarchy Level** [edit security certificates certification-authority]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Specify the certificate authority (CA) identity to use in the certificate request.

**Usage Guidelines** See "Specifying the Certificate Authority Name" on page 561.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## ca-profile

**Syntax**

```
ca-profile ca-profile-name {
    ca-identity ca-identity;
    enrollment {
        url url-name;
        retry number-of-enrollment-attempts;
        retry-interval seconds;
    }
    revocation-check {
        disable:
        crl {
            disable on-download-failure;
            refresh-interval number-of-hours;
            url {
                url-name;
                password;
            }
        }
    }
}
```

**Hierarchy Level** [edit security pki]

**Release Information** Statement introduced in JUNOS Release 7.5.
revocation-check and crl statements added in JUNOS Release 8.1.

**Description** Specify the name of the certificate authority (CA) profile for J-series Services Routers and Adaptive Services (AS) and MultiServices PICs installed on M-series and T-series routing platforms.

The remaining statements are explained separately.

**Options** *ca-profile-name*—Name of trusted CA.

**Usage Guidelines** See “Specifying the CA Profile Name” on page 574.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## cache-size

**Syntax** cache-size *bytes*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Configure the cache size for digital certificates.

**Options** *bytes*—Cache size for digital certificates.
**Range:** 64 through 4,294,967,295
**Default:** 2 megabytes (MB)

**NOTE:** We recommend that you limit your cache size to 4 MB.

**Usage Guidelines** See "Configuring the Cache Size" on page 563.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

## cache-timeout-negative

**Syntax** cache-timeout-negative *seconds*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Configure a negative cache for digital certificates.

**Options** *seconds*—Negative time to cache digital certificates, in seconds.
**Range:** 10 through 4,294,967,295
**Default:** 20

**CAUTION:** Configuring a large negative cache value can lead to a denial-of-service attack.

**Usage Guidelines** See "Configuring the Negative Cache" on page 563.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

## certificate-id

**Syntax**

```
certificate-id {
    ca-profile ca-profile-name;
    challenge-password password;
    re-enroll-trigger-time percentage;
    re-generate-keypair;
    validity-period days;
}
```

**Hierarchy Level** [edit security auto-re-enrollment]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** Specify a router certificate for auto-reenrollment. The ID is the same as that used to get the end entity's certificate from the issuing Certificate Authority.

**Usage Guidelines** See "Configuring the Auto-Reenrollment Properties" on page 580.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** auto-re-enrollment

## certificates

**Syntax**

```
certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
        ca-name ca-identity;
        crl file-name;
        encoding (binary | pem);
        enrollment-url url-name;
        file certificate-filename;
        ldap-url url-name;
    }
    enrollment-retry attempts;
    local certificate-name {
        certificate-key-string;
        load-key-file URL-or-path;
    }
    maximum-certificates number;
    path-length certificate-path-length;
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Configure the digital certificates for IPSec.

**Usage Guidelines** See “Configuring Digital Certificates (ES PIC)” on page 561.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## certification-authority

**Syntax**
```
certification-authority ca-profile-name {
    ca-name ca-identity;
    crl file-name;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
}
```

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Configure a certificate authority profile name. The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the Certificate Authority Properties" on page 561.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

## challenge-password

**Syntax** challenge-password *password*;

**Hierarchy Level** [edit security pki auto-re-enrollment certificate-id]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** Specify the challenge password used by the Certificate Authority (CA) for router certificate enrollment and revocation. This challenge password must be the same used when the router certificate was originally configured.

**Options** *password*—The password required by the CA.

**Usage Guidelines** See "Configuring the Auto-Reenrollment Properties" on page 580.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** auto-re-enrollment

## crl

See the following sections:



### *crl (Encryption Interface on M-series and T-series Routing Platforms Only)*

**Syntax** crl *file-name*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPSec peers on a regular periodic basis.

**Options** *file-name*—Specifies the file from which to read the CRL.

**Usage Guidelines** See "Configuring the Certificate Authority Properties" on page 561.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

## *crl (Adaptive Services Interfaces Only)*

**Syntax**

```
crl {
    disable on-download-failure;
    refresh-interval number-of-hours;
    url {
        url-name;
        password;
    }
}
```

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name* revocation-check]

**Release Information** Statement introduced in JUNOS Release 8.1.

**Description** Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPSec peers on a regular periodic basis.

**Options**

disable on-download-failure—Permits the authentication of the IPSec peer when the CRL is not downloaded.

refresh-interval *hours*—Time interval, in hours, between CRL updates.
**Range:** 0 through 8784
**Default:** 24

url *url-name*—Location from which to retrieve the CRL through the Lightweight Directory Access Protocol (LDAP). You can configure as many as three URLs for each configured CA profile.

**Usage Guidelines** See “Configuring the Certificate Revocation List” on page 575.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

## description

**Syntax** description *description*;

**Hierarchy Level** [edit security ike policy *ike-peer-address*],
[edit security ike proposal *ike-proposal-name*],
[edit security ipsec policy *ipsec-policy-name*],
[edit security ipsec proposal *ipsec-proposal-name*],
[edit security ipsec security-association *sa-name*]

**Description** Specify a text description for an IKE proposal or policy, or an IPSec proposal, policy, or SA.

**Usage Guidelines** See "Configuring Security Associations" on page 540, "Configuring the Description for an IKE Proposal" on page 549, "Configuring the Description for an IKE Policy" on page 551, "Configuring an IPSec Proposal (ES PIC)" on page 553, and "Configuring the IPSec Policy (ES PIC)" on page 555.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## dh-group

**Syntax** dh-group (group1 | group2);

**Hierarchy Level** [edit security ike proposal *ike-proposal-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the IKE Diffie-Hellman group.

**Options** dh-group—Type of Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. It can be one of the following:

- group1—768-bit.
- group2—1024-bit.

**Usage Guidelines** See "Configuring the Diffie-Hellman Group for an IKE Proposal" on page 549.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## direction

See the following sections:

- direction (JUNOS Software) on page 606
- direction (JUNOS-FIPS Software) on page 607

### *direction (JUNOS Software)*

**Syntax**

```
direction (inbound | outbound | bidirectional) {
    authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi auxiliary-spi-value;
    encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
}
```

**Hierarchy Level** [edit security ipsec security-association *sa-name* manual]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define the direction of IPSec processing.

**Options** inbound—Inbound SA.

outbound—Outbound SA.

bidirectional—Bidirectional SA.

**Usage Guidelines** See "Configuring the Processing Direction" on page 543.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *direction (JUNOS-FIPS Software)*

**Syntax**

```
direction (bidirectional | inbound | outbound) {
    protocol esp;
    spi spi-value;
    encryption {
        algorithm 3des-cbc;
        key ascii-text ascii-text-string;
    }
}
```

**Hierarchy Level** [edit security ipsec internal security-association manual]

**Description** Establish a manual security association (SA) for internal Routing-Engine-to-Routing-Engine communication.

**Options** bidirectional—Apply the same SA values in both directions between Routing Engines.

inbound—Apply these SA properties only to the inbound IPSec tunnel.

outbound—Apply these SA properties only to the outbound IPSec tunnel.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring Internal IPSec for JUNOS-FIPS” on page 588.

**Required Privilege Level** Crypto Officer—To view and add this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## dynamic

**Syntax**
```
dynamic {
    ipsec-policy ipsec-policy-name;
    replay-window-size (32 | 64);
}
```

**Hierarchy Level** [edit security ipsec security-association *name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define a dynamic IPSec SA.

**Options** ipsec-policy *ipsec-policy-name*—Name of the IPSec policy.

replay-window-size—(Optional) Antireplay window size. It can be one of the following values:

- 32—32-packet window size.
- 64—64-packet window size.

**Usage Guidelines** See "Configuring Dynamic Security Associations" on page 547 and "Configuring the ES PIC" on page 567.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## encoding

**Syntax** encoding (binary | pem);

**Hierarchy Level** [edit security ike policy *ike-peer-address*],
[edit security certificates certification-authority *ca-profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Specify the file format used for the local-certificate and local-key-pair statements.

**Options** binary—Binary file format.

pem—Privacy-enhanced mail (PEM), an ASCII base 64 encoded format.
**Default:** binary

**Usage Guidelines** See "Configuring the Type of Encoding Your CA Supports" on page 562 and "Configuring the Type of Encoding Your CA Supports" on page 565.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## encryption

See the following sections:

- encryption (JUNOS Software) on page 609
- encryption (JUNOS-FIPS Software) on page 610

### *encryption (JUNOS Software)*

**Syntax**

```
encryption {
    algorithm (des-cbc | 3des-cbc);
    key (ascii-text key | hexadecimal key);
}
```

**Hierarchy Level** [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bidirectional)]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure an encryption algorithm and key for manual SA.

**Options** algorithm—Type of encryption algorithm. It can be one of the following:

- des-cbc—Has a block size of 8 bytes (64 bits); its key size is 48 bits long.
- 3des-cbc—Has block size of 8 bytes (64 bits); its key size is 192 bits long.

**NOTE:** For 3des-cbc, we recommend that the first 8 bytes be different from the second 8 bytes, and the second 8 bytes be the same as the third 8 bytes.

key—Type of encryption key. It can be one of the following:

- ascii-text—ASCII text key. For the des-cbc option, the key contains 8 ASCII characters; for 3des-cbc, the key contains 24 ASCII characters.
- hexadecimal—Hexadecimal key. For the des-cbc option, the key contains 16 hexadecimal characters; for the 3des-cbc option, the key contains 48 hexadecimal characters.

**Usage Guidelines** See "Configuring the Encryption Algorithm and Key" on page 546.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

### *encryption (JUNOS-FIPS Software)*

**Syntax**
```
encryption {
    algorithm 3des-cbc;
    key ascii-text ascii-text-string;
}
```

**Hierarchy Level** [edit security ipsec internal security-association manual direction]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define the encryption parameters for internal Routing-Engine-to-Routing-Engine communication. The remaining statements are explained separately.

**Usage Guidelines** See "Configuring Internal IPSec for JUNOS-FIPS" on page 588.

**Required Privilege Level** Crypto Officer—To view and add this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## encryption-algorithm

**Syntax** encryption-algorithm (3des-cbc | des-cbc | ase-128-cbc | ase-192-cbc | ase-256-cbc);

**Hierarchy Level** [edit security ike proposal *ike-proposal-name*],
[edit security ipsec proposal *ipsec-proposal-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure an IKE or IPSec encryption algorithm.

**Options**

3des-cbc—Encryption algorithm with key size of 24 bytes; its key size is 192 bits long.

des-cbc—Encryption algorithm with key size of 8 bytes; its key size is 48 bits long.

aes-128-cbc—Advanced encryption algorithm that has a key size of 16 bytes; its key size is 128 bits long.

aes-192-cbc—Advanced encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.

aes-256-cbc—Advanced encryption algorithm that has a key size of 32 bytes; its key size is 256 bits long.

**Usage Guidelines** See "Configuring the Encryption Algorithm for an IKE Proposal" on page 550 and "Configuring the Encryption Algorithm for an IPSec Proposal" on page 554.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## enrollment

**Syntax**

```
enrollment {
    url url-name;
    retry number-of-enrollment-attempts;
    retry-interval seconds;
}
```

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name*]

**Release Information** Statement introduced in JUNOS Release 7.5.

**Description** Specify the URL and enrollment parameters of the certificate authority (CA) for J-series Services Routers and Adaptive Services (AS) and MultiServices PICs installed on M-series and T-series routing platforms.

**Options**

url *url-name*—Location of CA to which the router sends the Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests for the configured CA profile. Use the CA host DNS name or IP address.

retry *number-of-enrollment-attempts*—Number of enrollment retries.
**Range:** 0 through 100
**Default:** 0

retry-interval *seconds*—Amount of time, in seconds, a router should wait between enrollment attempts.
**Range:** 0 through 3600
**Default:** 0

**Usage Guidelines** See "Specifying an Enrollment URL" on page 575 and "Specifying the Enrollment Properties" on page 575.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## enrollment-retry

**Syntax** enrollment-retry *attempts*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Specify how many times a router can resend a digital certificate request.

**Options** *attempts*—Number of enrollment retries.
**Range:** 0 through 100
**Default:** 0

**Usage Guidelines** See "Configuring the Number of Enrollment Retries" on page 564.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## enrollment-url

**Syntax** enrollment-url *url-name*;

**Hierarchy Level** [edit security certificates certification-authority *ca-profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Specify where your router should send Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).

**Options** *url-name*—Certificate authority URL.

**Usage Guidelines** See "Specifying an Enrollment URL" on page 562.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## file

**Syntax** file *certificate-filename*;

**Hierarchy Level** [edit security certificates certification-authority *ca-profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Specify the file from which to read the digital certificate.

**Options** *certificate-filename*—File from which to read the digital certificate.

**Usage Guidelines** See "Specifying a File to Read the Digital Certificate" on page 563.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## identity

**Syntax** identity *identity-name*;

**Hierarchy Level** [edit security ike]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define the identity of the remote certificate name if the identity cannot be learned through IKE (ID payload or IP address).

**Usage Guidelines** See "Configuring the Identity to Define the Remote Certificate Name" on page 566.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## ike

**Syntax**

```
ike {
    policy ike-peer-address {
        description policy-description;
        encoding (binary | pem);
        identity identity-name;
        local-certificate certificate-filename;
        local-key-pair private-public-key-file;
        mode (aggressive | main);
        pre-shared-key (ascii-text key | hexadecimal key);
        proposals [ proposal-names ];
    }
    proposal ike-proposal-name {
        authentication-algorithm (md5 | sha1);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        dh-group (group1 | group2);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
    }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Configure IKE.

The statements are explained separately.

**Usage Guidelines** See "Configuring an IKE Proposal (Dynamic SAs Only)" on page 548 and "Configuring an IKE Policy for Preshared Keys" on page 550.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## internal

**Syntax**

```
internal {
   security-association {
      manual {
         direction (bidirectional | inbound | outbound) {
            protocol esp;
            spi spi-value;
            encryption {
               algorithm 3des-cbc;
               key ascii-text ascii-text-string;
            }
         }
      }
   }
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (JUNOS-FIPS only) Define an internal security association (SA) for internal Routing-Engine-to-Routing-Engine communication. The remaining statements are explained separately.

**Usage Guidelines** See “Configuring Internal IPSec for JUNOS-FIPS” on page 588.

**Required Privilege Level** Crypto Officer—To view and add this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## ipsec

**Syntax**

```
ipsec {
    security-association {
        manual {
            direction (bidirectional | inbound | outbound) {
                protocol esp;
                spi spi-value;
                encryption {
                    algorithm 3des-cbc;
                    key ascii-text ascii-text-string;
                }
            }
        }
    }
    policy ipsec-policy-name {
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposals [ proposal-names ];
    }
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol (ah | esp | bundle);
    }
    security-association name {
        dynamic {
            ipsec-policy policy-name;
            replay-window-size (32 | 64);
        }
        manual {
            direction (inbound | outbound | bi-directional) {
                authentication {
                    algorithm (hmac-md5-96 | hmac-sha1-96);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi auxiliary-spi-value;
                encryption {
                    algorithm (des-cbc | 3des-cbc);
                    key (ascii-text key | hexadecimal key);
                }
                protocol (ah | esp | bundle);
                spi spi-value;
            }
        }
        mode (tunnel | transport);
    }
    traceoptions {
        file <files number> < size size>;
        flag all;
        flag database;
```

```
        flag general;
        flag ike;
        flag parse;
        flag policy-manager;
        flag routing-socket;
        flag timer;
    }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Configure IPSec.

The statements are explained separately.

**Usage Guidelines** See "Configuring Security Associations" on page 540.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## key

**Syntax** key ascii-text *ascii-text-string*;

**Hierarchy Level** [edit security ipsec internal security-association manual direction encryption]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** The key used for the internal Routing-Engine-to-Routing-Engine IPSec security association (SA) configuration.

**Options** Only ascii-text is supported.

*ascii-text-string*—The encrypted ASCII text key.

**Usage Guidelines** See "Configuring Internal IPSec for JUNOS-FIPS" on page 588.

**Required Privilege Level** Crypto Officer—To add and view this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## ldap-url

**Syntax** ldp-url *url-name*;

**Hierarchy Level** [edit security certificates certification-authority *ca-profile-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platform only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.

**Options** *url-name*—Name of the LDAP URL.

**Usage Guidelines** See "Specifying an LDAP URL" on page 563.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## lifetime-seconds

**Syntax** lifetime-seconds *seconds*;

**Hierarchy Level** [edit security ike proposal *ike-proposal-name*],
[edit security ipsec proposal *ipsec-proposal-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Optional) Configure the lifetime of IKE or IPSec SA. When the SA expires, it is replaced by a new SA (and SPI) or terminated.

**Options** *seconds*—Lifetime, in seconds.
**Range:** 180 through 86,400

**Usage Guidelines** See "Configuring the Lifetime for an IKE SA" on page 550 and "Configuring the Lifetime for an IPSec SA" on page 555.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## local

**Syntax**
```
local certificate-name {
    certificate-key-string;
    load-key-file URL-or-path;
}
```

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Import a paired X.509 private key and authentication certificate, to enable JUNOScript client applications to establish Secure Sockets Layer (SSL) connections to the router.

**Options** *certificate-key-string*—String of alphanumeric characters that constitute the private key and certificate.

*certificate-name*—Name that uniquely identifies the certificate.

load-key-file—File that contains the private key and certificate. It can be one of two types of values:

- Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's local disk)
- URL to the certificate file location (for instance, on the computer where the JUNOScript client application runs)

**Usage Guidelines** See "Importing SSL Certificates for JUNOScript Support" on page 587.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## local-certificate

**Syntax** local-certificate *certificate-filename*;

**Hierarchy Level** [edit security ike policy *ike-peer-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the certificate filename from which to read the local certificate.

**Options** *certificate-filename*—File from which to read the local certificate.

**Usage Guidelines** See "Specifying the Certificate Filename" on page 566.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## local-key-pair

**Syntax** local-key-pair *private-public-key-file*;

**Hierarchy Level** [edit security ike policy *ike-peer-address*]

**Release Information** Statement introduced before JUNOS 7.4.

**Description** Specify private and public keys.

**Options** *private-public-key-file*—Specifies the file from which to read the private and public key pair.

**Usage Guidelines** See "Specifying the Private and Public Key File" on page 566.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## manual

See the following sections:

- manual (JUNOS Software) on page 621
- manual (JUNOS-FIPS Software) on page 622

### *manual (JUNOS Software)*

**Syntax**

```
manual {
   direction (inbound | outbound | bi-directional) {
      authentication {
         algorithm (hmac-md5-96 | hmac-sha1-96);
         key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi auxiliary-spi-value;
      encryption {
         algorithm (des-cbc | 3des-cbc);
         key (ascii-text key | hexadecimal key);
      }
      protocol (ah | esp | bundle);
      spi spi-value;
   }
}
```

**Hierarchy Level** [edit security ipsec security-association]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define a manual IPSec SA.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring Manual Security Associations” on page 543.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *manual (JUNOS-FIPS Software)*

**Syntax**
```
manual {
    direction (bidirectional | inbound | outbound) {
        protocol esp;
        spi spi-value;
        encryption {
            algorithm 3des-cbc;
            key ascii-text ascii-text-string;
        }
    }
}
```

**Hierarchy Level** [edit security ipsec internal security-association]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define a manual security association (SA) for internal Routing-Engine-to-Routing-Engine communication.

**Options** The remaining statements are explained separately.

**Usage Guidelines** See “Configuring Internal IPSec for JUNOS-FIPS” on page 588.

**Required Privilege Level** Crypto Officer—To view and add this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## maximum-certificates

**Syntax** maximum-certificates *number*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platforms only) Configure the maximum number of peer digital certificates to be cached.

**Options** *number*—Maximum number of peer digital certificates to be cached.
**Range:** 64 through 4,294,967,295 peer certificates
**Default:** 1024 peer certificates

**Usage Guidelines** See “Configuring the Maximum Number of Peer Certificates” on page 564.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## mode

See the following sections:

- mode (IKE) on page 623
- mode (IPSec) on page 624

### *mode (IKE)*

**Syntax** mode (aggressive | main);

**Hierarchy Level** [edit security ike policy *ike-peer-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define the IKE policy mode.

**Default** main

**Options** aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection.

main—Uses six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection.

**Usage Guidelines** See "Configuring the Mode for an IKE Policy" on page 551.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *mode (IPSec)*

**Syntax** mode (transport | tunnel);

**Hierarchy Level** [edit security ipsec security-association *name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define the mode for the IPSec security association.

**Default** tunnel

**Options** transport— Protects traffic when the communication endpoint and cryptographic endpoint are the same. The data portion of the IP packet is encrypted, but the IP header is not. Virtual Private Network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications.

tunnel—Protects traffic using preshared keys with IKE to authenticate peers or digital certificates with IKE to authenticate peers.

**NOTE:** Tunnel mode requires the ES Physical Interface Card (PIC).

The JUNOS software supports only encapsulating security payload (ESP) when you use tunnel mode.

In transport mode, the JUNOS software does not support authentication header (AH) and ESP header bundles.

In transport mode, the JUNOS software supports only Border Gateway Protocol (BGP).

**Usage Guidelines** See “Configuring IPSec Mode” on page 541.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## path-length

**Syntax** path-length *certificate-path-length*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Encryption interface on M-series and T-series routing platform only) Configure the digital certificate path length.

**Options** *certificate-path-length*—Digital certificate path length.
**Range:** 2 through 15 certificates
**Default:** 15 certificates

**Usage Guidelines** See "Configuring the Path Length for the Certificate Hierarchy" on page 564.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## perfect-forward-secrecy

**Syntax**
```
perfect-forward-secrecy {
   keys (group1 | group2);
}
```

**Hierarchy Level** [edit security ipsec policy *ipsec-policy-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Optional) Define the Perfect Forward Secrecy (PFS) protocol. Creates single-use keys.

**Options** keys—Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange.

The key can be one of the following:

- group1—768-bit.
- group2—1024-bit.

**Usage Guidelines** See "Configuring Perfect Forward Secrecy" on page 556.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## pki

**Syntax**

```
pki {
    ca-profile ca-profile-name {
        ca-identity ca-identity;
        enrollment {
            url url-name;
            retry number-of-enrollment-attempts;
            retry-interval seconds;
        }
        revocation-check {
            disable;
            crl {
                disable on-download-failure;
                refresh-interval hours;
                url {
                    url-name;
                    password;
                }
            }
        }
    }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in JUNOS Release 7.5.
revocation-check and crl statements added in JUNOS Release 8.1.

**Description** Configure an IPSec profile to request digital certificates for J-series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M-series and T-series routing platforms.

The statements are explained separately.

**Usage Guidelines** See "Configuring Digital Certificates for Adaptive Services Interfaces" on page 573.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** *JUNOS Feature Guide* and the *JUNOS System Basics and Services Command Reference*

## policy

See the following sections:



### *policy (IKE)*

**Syntax**

```
policy ike-peer-address {
   description policy-description;
   encoding (binary | pem);
   identity identity-name;
   local-certificate certificate-filename;
   local-key-pair private-public-key-file;
   mode (aggressive | main);
   pre-shared-key (ascii-text key | hexadecimal key);
   proposals [ proposal-names ];
}
```

**Hierarchy Level** [edit security ike]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define an IKE policy.

**Options** *ike-peer-address*—A tunnel address configured at the [edit interfaces es] hierarchy level.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring an IKE Policy for Preshared Keys" on page 550 and "Configuring an IKE Policy for Digital Certificates (ES PIC)" on page 565.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *policy (IPSec)*

**Syntax**
```
policy ipsec-policy-name {
   perfect-forward-secrecy {
      keys (group1 | group2);
   }
   proposals [ proposal-names ];
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define an IPSec policy.

**Options** *ipsec-policy-name*—Specify an IPSec policy name.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the IPSec Policy (ES PIC)" on page 555.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## pre-shared-key

**Syntax** pre-shared-key (ascii-text *key* | hexadecimal *key*);

**Hierarchy Level** [edit security ike policy *ike-peer-address*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation. Specify the key in either ASCII or hexadecimal format.

**Options** ascii-text *key*—Authentication key in ASCII format.

hexadecimal *key*—Authentication key in hexadecimal format.

**Usage Guidelines** See "Configuring the Preshared Key for an IKE Policy" on page 552.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

# proposal

See the following sections:

- proposal (IKE) on page 629
- proposal (IPSec) on page 630

## *proposal (IKE)*

**Syntax**

```
proposal ike-proposal-name {
    authentication-algorithm (md5 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2);
    encryption-algorithm (3des-cbc | des-cbc);
    lifetime-seconds seconds;
}
```

**Hierarchy Level** [edit security ike]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define an IKE proposal for a dynamic SA.

**Options** *ike-proposal-name*—Specifies an IKE proposal name.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring an IKE Proposal (Dynamic SAs Only)" on page 548.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *proposal (IPSec)*

**Syntax**
```
proposal ipsec-proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    encryption-algorithm (3des-cbc | des-cbc);
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define an IPSec proposal for a dynamic SA.

**Options** *ipsec-proposal-name*—Specifies an IPSec proposal name.

The statements are explained separately.

**Usage Guidelines** See "Configuring an IPSec Proposal (ES PIC)" on page 553.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## proposals

**Syntax** proposals [ *proposal-names* ];

**Hierarchy Level** [edit security ike policy *ike-peer-address*],
[edit security ipsec policy *ipsec-policy-name*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Associate one or more proposals with an IKE or IPSec policy.

**Options** *proposal-names*—Name of one or more proposals.

**Usage Guidelines** See "Associating Proposals with an IKE Policy" on page 552 and "Configuring the IPSec Policy (ES PIC)" on page 555.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## protocol

See the following sections:



### *protocol (JUNOS Software)*

**Syntax** protocol (ah | esp | bundle);

**Hierarchy Level** [edit security ipsec proposal *ipsec-proposal-name*],
[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bidirectional)]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define the IPSec protocol for a manual or dynamic SA.

**Options** ah—Authentication Header protocol

bundle—AH and ESP protocols

esp—ESP protocol (the tunnel statement must be included at the [edit security ipsec security-association *sa-name* mode hierarchy level)

**Usage Guidelines** See "Configuring the Protocol for a Manual SA" on page 544 and "Configuring the Protocol for a Dynamic IPSec SA" on page 555.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

### *protocol (JUNOS-FIPS Software)*

**Syntax** protocol esp;

**Hierarchy Level** [edit security ipsec internal security-association manual direction]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** The protocol used for the internal Routing-Engine-to-Routing-Engine IPSec security association (SA) configuration.

**Options** Only esp is supported.

**Usage Guidelines** See "Configuring Internal IPSec for JUNOS-FIPS" on page 588.

**Required Privilege Level** Crypto Officer—To add and view this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## re-enroll-trigger-time

**Syntax** re-enroll-trigger-time *percentage*;

**Hierarchy Level** [edit security pki auto-re-enrollment certificate-id]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** Percentage of the router certificate validity-period statement value, in days, when auto-reenrollment should start before expiration.

**Options** *percentage*—Percentage for the reenroll trigger time.
**Range:** 1 through 99

**Usage Guidelines** See "Configuring the Auto-Reenrollment Properties" on page 580.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** auto-re-enrollment

## re-generate-keypair

**Syntax** re-generate-keypair;

**Hierarchy Level** [edit security pki auto-re-enrollment certificate-id]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** (Optional) Automatically generate a new key pair when auto-reenrolling a router certificate. If this statement is not configured, the current key pair is used.

**Usage Guidelines** See "Configuring the Auto-Reenrollment Properties" on page 580.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** auto-re-enrollment

## refresh-interval

**Syntax** refresh-interval *hours*;

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name* revocation-check crl]

**Release Information** Statement introduced in JUNOS Release 8.1.

**Description** (Adaptive services interfaces only) Specify the amount of time between certificate revocation list (CRL) updates.

**Options** *number-of-hours*—Time interval, in hours, between CRL updates.
**Range:** 0 through 8784
**Default:** 24

**Usage Guidelines** "Configuring the Certificate Revocation List" on page 575.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** crl

## retry

**Syntax** retry *number-of-attempts*;

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name* enrollment]

**Release Information** Statement introduced in JUNOS Release 7.5.

**Description** (Adaptive services interfaces only) Specify how many times a router can resend a digital certificate request.

**Options** *number-of-attempts*—Number of enrollment retries.
**Range:** 0 through 100
**Default:** 0

**Usage Guidelines** See "Specifying the Enrollment Properties" on page 575.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** enrollment

## retry-interval

**Syntax** retry-interval *seconds*;

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name* enrollment]

**Release Information** Statement introduced in JUNOS Release 7.5.

**Description** (Adaptive services interfaces only) Specify the amount of time the router should wait between enrollment retries.

**Options** *seconds*—Time interval, in seconds, between enrollment retries.
**Range:** 0 through 3600
**Default:** 0

**Usage Guidelines** See "Specifying the Enrollment Properties" on page 575.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** enrollment

## revocation-check

**Syntax**

```
revocation-check {
    disable;
    crl {
        refresh-interval number-of-hours;
        url {
            url-name;
        }
    }
}
```

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name*]

**Release Information** Statement introduced in JUNOS Release 8.1.

**Description** Specify the method to verify revocation status of digital certificates for J-series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M-series and T-series routing platforms.

**Options**

disable—Disable verification of status of digital certificates.

crl—Only certificate revocation list (CRL) is supported. A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPSec peers on a regular periodic basis. By default, crl is enabled.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the Certificate Revocation List" on page 575.

**Required Privilege Level**

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## security-association

See the following sections:

- security-association (JUNOS Software) on page 636
- security-association (JUNOS-FIPS Software) on page 637

### *security-association (JUNOS Software)*

**Syntax**

```
security-association sa-name {
    dynamic {
        ipsec-policy policy-name;
        replay-window-size (32 | 64);
    }
    manual {
        direction (JUNOS Software) (inbound | outbound | bi-directional) {
            authentication {
                algorithm (hmac-md5-96 | hmac-sha1-96);
                key (ascii-text key | hexadecimal key);
            }
            auxiliary-spi auxiliary-spi-value;
            encryption {
                algorithm (des-cbc | 3des-cbc);
                key (ascii-text key | hexadecimal key);
            }
            protocol ( ah | esp | bundle);
            spi spi-value;
        }
        mode (tunnel | transport);
    }
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure an IPSec security association.

**Options** *name*—Name of the security association.

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring Security Associations" on page 540.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## *security-association (JUNOS-FIPS Software)*

**Syntax**

```
security-association {
    manual {
        direction (bidirectional | inbound | outbound) {
            protocol esp;
            spi spi-value;
            encryption {
                algorithm 3des-cbc;
                key ascii-text ascii-text-string;
            }
        }
    }
}
```

**Hierarchy Level** [edit security ipsec internal]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Define a security association (SA) for internal Routing-Engine-to-Routing-Engine communication.

**Options** The remaining statements are explained separately.

**Usage Guidelines** See “Configuring Internal IPSec for JUNOS-FIPS” on page 588.

**Required Privilege Level** Crypto Officer—To view and add this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## spi

See the following sections:



### *spi (JUNOS Software)*

**Syntax** spi *spi-value*;

**Hierarchy Level** [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure SPI for an SA.

**Options** *spi-value*—An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).
**Range:** 256 through 16639

**NOTE:** Use the auxiliary SPI when you configure the protocol statement to use the bundle option.

**Usage Guidelines** See "Configuring the Security Parameter Index" on page 545.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

### *spi (JUNOS-FIPS Software)*

**Syntax** spi *spi-value*;

**Hierarchy Level** [edit security ipsec internal security-association manual direction]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** The Security Parameter Index (SPI) value used for the internal Routing-Engine-to-Routing-Engine IPSec security association (SA) configuration.

**Options** *spi-value*—Integer to use for this SPI.
**Range:** 256 through 16639

**Usage Guidelines** See "Configuring Internal IPSec for JUNOS-FIPS" on page 588.

**Required Privilege Level** Crypto Officer—To add and view this statement in the configuration.

**Related Topics** *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*

## ssh-known-hosts

**Syntax**

```
ssh-known-hosts {
    host {
        dsa-key key;
        rsa-key key;
        rsa1-key key;
    }
}
```

**Hierarchy Level** [edit security ssh-known-hosts]

**Release Information** Statement introduced in JUNOS Release 7.5.

**Description** Configure SSH support for known hosts and for administering for SSH host key updates.

**Options**

dsa-key—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.

rsa-key—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.

rsa1-key—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.

fetch-from-server—Retrieve SSH public host key information from a specified server.

load-key-file—Import SSH host key information from the /var/tmp/ssh-known-hosts file.

**Usage Guidelines** See “Configuring SSH Host Keys for Secure Copy” on page 584.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## traceoptions

**Syntax**

```
traceoptions {
    file filename <files number> <size size>;
    flag all;
    flag database;
    flag general;
    flag ike;
    flag parse;
    flag policy-manager;
    flag routing-socket;
    flag timer;
}
```

**Hierarchy Level** [edit security],
[edit services ipsec-vpn]

Trace options can be configured at either the [edit security] or the [edit services ipsec-vpn] hierarchy level, but not at both levels.

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure security trace options.

To specify more than one trace option, include multiple flag statements. Trace option output is recorded in the /var/log/kmd file.

**Options**

files *number*—(Optional) Maximum number of trace files. When a trace file (for example, kmd) reaches its maximum size, it is renamed kmd.0, then kmd.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the size option.
**Range:** 2 through 1000 files
**Default:** 0 files

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, kmd) reaches this size, it is renamed, kmd.0, then kmd.1 and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
**Default:** 1024 KB

*flag*—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

- all—Trace all security events.
- database—Trace database events.
- general—Trace general events.

- ike—Trace IKE module processing.
- parse—Trace configuration processing.
- policy-manager—Trace policy manager processing.
- routing-socket—Trace routing socket messages.
- timer—Trace internal timer events.

**Usage Guidelines** See "Configuring Trace" on page 582.

**Required Privilege Level** admin—To view the configuration.
admin-control—To add this statement to the configuration.

## url

**Syntax** url *url-name*;

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name* enrollment],
[edit security pki ca-profile *ca-profile-name* revocation-check crl]

**Release Information** Statement introduced in JUNOS Release 7.5.

**Description** (Adaptive services interfaces only) Specify the certificate authority (CA) URL to use in requesting digital certificates or the URL for the Lightweight Access Directory Protocol (LDAP) location from which retrieve the certificate revocation list (CRL).

**Options** *url-name*—URL of CA or URL of LDAP location of CRL.

**Usage Guidelines** See "Specifying an Enrollment URL" on page 575 and "Specifying an LDAP URL" on page 576.

**Required Privilege Level** admin—To view the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** enrollment

crl

## validity-period

**Syntax** validity-period *days*;

**Hierarchy Level** [edit security pki auto-re-enrollment certificate-id]

**Release Information** Statement introduced in JUNOS Release 8.5.

**Description** (Optional) Certificate validity period, in days, from the enrollment start date. If not specified, the issuing certificate authority (CA) sets this time as per its own policy. The start time is when auto-reenrollment is initiated.

**Options** *days*—Number of days that the certificate is valid.
**Range:** 1 through 4095 days
**Default:** Per CA policy

**Usage Guidelines** See "Configuring the Auto-Reenrollment Properties" on page 580

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Topics** auto-re-enrollment

# Part 5
# JUNOS Software Development Kit

Chapter 18

# SDK Applications Overview

The JUNOS Software Development Kit (SDK) allows members of the Juniper Open IP Solution Development Program (OSDP) to build custom applications that run on the JUNOS operating system and extend the functionality of JUNOS systems. Such an application may run on the Routing Engine or, to perform a specific service, on the MultiServices PIC. In JUNOS user documentation, these third-party applications are called *SDK applications*. These applications are installed in one or more packages.

The material in this part pertains only to configuring routers that run SDK applications. If you have no SDK applications on your router, you can disregard this and the next three chapters.

A JUNOS SDK application may already be on your router if it was provided to you by a third party, or you may need to install the SDK application if you acquired it separately from the router.

To install an SDK application, please consult the application-specific documentation supplied by the provider. The application-specific documentation may also have information about configuring the SDK application on the router that is in addition to the generic information in these chapters.

In the configuration itself, the SDK application is called an *extension*, and the third-party creator of that application is called a *provider*. Also specific to SDK applications is the SDK service process, or ssd. This process, which runs on the Routing Engine, is responsible for communications between the SDK application and the regular JUNOS software. Although ssd is present on the router, it does not run unless specifically enabled, as described in the section "Enabling the SDK Service Process and SDK Application Deployment" on page 647.

For security, an SDK application comes with a certificate that authenticates it as a product of a specific provider. Part of this certificate, the *provider ID*, must be activated on the router to allow the SDK application to be deployed on the router and run.

If an SDK application will run on the MultiServices PIC, which is based on a multicore chip, you can designate the number of cores used for control versus data handling. Your application provider may recommend values for this core allocation, or you may choose these values yourself.

For more information about the Juniper OSDP and the JUNOS SDK, please contact your account team or visit http://www.juniper.net/partners/osdp.html.

Chapter 19

# SDK Applications Configuration Guidelines

The material in this chapter pertains only to configuring routers that run JUNOS SDK applications.

The following sections describe how to configure, display, and modify your system for operation with JUNOS SDK applications:



## Enabling the SDK Service Process and SDK Application Deployment

By default, the SDK service process (ssd) does not run. You enable ssd and prepare the router for installation of a JUNOS SDK application by including the following statements at the [edit system] hierarchy level:

```
[edit]
system {
    extensions {
        providers {
            provider-id;
        }
    }
}
```

The provider ID is a prefix that is part of the certificate name used by the provider in building an SDK application. Before installing your SDK application, you must enable its provider ID using the extensions statement. Enabling a provider ID allows you to install the SDK application package that was built using that certificate name. Multiple provider IDs can be enabled on a router.

### *Example: extensions Statement*

If abc and xyz are provider IDs issued to two providers, then the following configuration enables the router for the SDK applications built by either provider:

```
[edit]
system {
   extensions {
      providers {
         abc;
         xyz;
      }
   }
}
```

## Configuring the MultiServices PIC

To configure an SDK application, include the following statements at the [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number adaptive-services service-package
   extension-provider]
control-cores control-number;
data-cores data-number;
forwarding-db-size size;
object-cache-size value;
package package-name;
policy-db-size size;
wired-process-mem-size size;
syslog {
   facility severity;
}
```

There are eight cores in a PIC. Some cores, called *control cores*, are dedicated to running control functionality for the application. Cores dedicated to processing data for the application are called *data cores*. You must designate at least one core as a control core. Although it is not mandatory to designate any cores as data cores, it is advisable to designate a minimum of five, depending on the nature of the application, to achieve good performance. The total number of cores, both control and data cores, that you can dedicate using the extension-provider statement ranges from one through eight. Any cores not configured as control or data cores are treated as *user cores*.

**NOTE:** For help with architecting your application, consult with JUNOS SDK Developer Support.

The MultiServices PIC has a shared memory pool that contains the object cache and the forwarding database (FDB). The FDB provides access to the route information. It is a separate memory derived from the object cache shared memory on the MultiServices PIC.

A large FDB implies there is less object cache for the application, which can affect performance depending on the application. For example, if an application needs a maximum of 256 MB of object cache for its functionality and the value of object-cache-size is 512 MB, the object cache can allocate up to 256 MB to the FDB without any performance impact. However, if the value set for object-cache-size is only 256 MB and forwarding-db-size is set to 64MB, there will be some performance impact.

**NOTE:** You need to enable forwarding options sampling for the FDB to be created. For information about enabling sampling, see "Enabling Sampling on a MultiServices PIC" on page 655.

To tune SDK application performance, use the object-cache-size statement, specifying a value that is a multiple of 128 megabytes (MB). For the MS-100 PIC, the range is from 128 through 512 MB, and for the MS-400 PIC, from 128 through 1280 MB.

**NOTE:** Changing the object cache size on a running system causes the PIC to reboot.

JUNOS SDK applications are installed on the MultiServices PIC in one or more packages. To designate which SDK application package to install on a given PIC, include the package *package-name* option. Up to eight packages can be installed on a PIC; however, only one data package is allowed per PIC.

**NOTE:** You cannot install both a JUNOS service package and an SDK application package on the same PIC.

You cannot install more than one SDK application on a PIC.

The policy-db-size statement defines the size of policies that providers expect to be present in their system. It is configured in megabytes. The size should be less than that set for the object-cache-size statement.

To record or view system log messages on a specific PIC, include the syslog statement. System log information is passed to the Routing Engine and put in the /var/log/messages directory. Two facilities are supported: external and pfe. The pfe facility logs actions performed or errors encountered by the Packet Forwarding Engine. The external facility covers everything outside of the Packet Forwarding Engine. Severity is the same as for the JUNOS software; see Table 20 on page 116 for the severity levels that you can specify.

Wired process memory is memory used by the operating system that is generally "off limits" to another application. To configure wired process memory size, specify 512 MB for the wired-process-mem-size statement. In addition, you can also configure the object cache.

### *Example: extension-provider Statement*

In the following example, several PIC configurations are demonstrated. All but one of the available cores are configured. Three cores are control cores, four are data cores, and one is a user core.

```
[edit]
chassis {
   fpc 0 {
      pic 1 {
         adaptive-services {
            service-package {
               extension-provider {
                  control-cores 1;
                  data-cores 6;
                  forwarding-db-size 128;
                  object-cache-size 768;
                  package jnx-flow-data;
                  policy-db-size 128;
                  wired-process-mem-size 512;
               }
            }
         }
      }
   }
}
```

## Configuring SDK Service Sets

This section explains the use of service sets in SDK applications. For more information about service sets, see the *JUNOS Services Interfaces Configuration Guide*.

A service set is a collection of policies taken from multiple services that can be applied as a unit to traffic coming to the PIC. Service sets are the building blocks of SDK plug-ins. Currently, up to two SDK plug-ins are supported per PIC.

Policies are maintained per service set only. For defining policies using the command-line interface (CLI), the SDK does not specify how providers must set up the configuration hierarchy. However, two things are mandatory:

- Service sets must be configured at the [edit services service-set *service-set-name* extension-service] hierarchy level.
- The service-order statement must be used to specify the order in which policies are applied to traffic coming to the PIC.

To specify the order of the policies within a service set, configure the service-order statement at the [edit services extension-service] hierarchy level.

To define a service set, configure statements at the [edit services service-set *service-set-name* extension-service] hierarchy level. For specific information, see the application-specific documentation.

SDK application providers may want to follow the JUNOS software method of configuring a service set. In the native JUNOS software, policies known as “rules” or groups of rules known as “rule sets” are configured at the [edit services] hierarchy level. These services are then gathered together in a service set at the [edit services service-set *service-set-name* extension-service] hierarchy level by referencing the names of the rules or rule sets.

The following sections briefly explain service sets as they relate to SDK applications:


- Service Order on page 651
- Interface and Next-Hop Service Sets on page 653
- Limitations and Constraints for SDK Services Sets on page 654


## *Service Order*

The service order defines the order in which services are applied for this service set. The service-order statement must include all services defined in the service set. It is mandatory to specify the forward-flow service order and the reverse-flow service flow. If the reverse-flow service order is not specified, the reverse-flow order is the reverse of the forward-flow service-order.

To configure the service order, include the service-order statement at the [edit services service-set *service-set-name* extension-service] hierarchy level.

**NOTE:** If the extension-service statement is specified, the service-order statement is mandatory. Service order should not be configured for native JUNOS internal services. For the internal services, there is a default service order that is assumed.

To change the service order, delete the service order elements and then add them again in the new order.

### Example: Service Set Configuration

In following configuration example, the acme-svc1 service is defined by three rules (content unspecified) and the acme-svc2 service is defined by a rule set made up of an unspecified number of rules. In this case, these services are defined at the [edit acme services] hierarchy level.

```
[edit]
acme {
   services {
      acme-svc1 { #Provider-defined service
         svc1-rule1 { # First rule’s name
            . . . # First rule defined
         }
         svc1-rule2 { # Second rule’s name
            . . . # Second rule defined
         }
         svc1-rule3 { # Third rule’s name
            . . . # Third rule defined
         }
```

```
        }
        acme-svc2 { # Provider-defined service
            rule-set svc2-rule-set {# Rule-set name
                [ rules rule-names ]; # Rules definitions start here
            }
        }
    }
}
```

At the [edit services] hierarchy level (no intervening "acme" level here), the service-set *sset1* is defined by referencing the three rule names for acme-svc1 and the one rule set name for acme-svc2 using the service-set *service-set-name* extension-service statement at the [edit services service-set *service-set-name*] hierarchy level. The service order is also configured at the [edit services service-set *service-set-name*] hierarchy level.

The following is an example of configuring service sets, extension service rules, and the service order:

```
[edit]
services {
    service-set sset1 {
        extension-service acme-svc1 {
            svc1-rule1;
            svc1-rule2;
            svc1-rule3;
        }
        extension-service acme-svc2 {
            rule-set svc2-rule-set;
        }
        /* Now define the order */
        service-order {
            forward-flow [acme-svc1 acme-svc2];
            reverse-flow [acme-svc1 acme-svc2];
        }
    }
}
```

### Example: Service Order Configuration

The following is another example of configuring the service order:

```
[edit]
services {
    service-set sset1 {
        next-hop-service {
            inside-service-interface ms-5/0/0.1;
            outside-service-interface ms-5/0/0.2;
            }
            extension-service jnx-msptest-plugin2;
            extension-service jnx-msptest-plugin1;
            service-order {
                forward-flow [ jnx-msptest-plugin1 jnx-msptest-plugin2 ];
                reverse-flow [ jnx-msptest-plugin1 jnx-msptest-plugin2 ];
            }
```

```
    }
  }
}
```

### *Interface and Next-Hop Service Sets*

There are two types of service sets: interface and next-hop. Interface service sets must be attached to media interfaces to direct traffic to the PIC, and they apply to all packets entering and leaving the PIC. After the service set is applied, packets can be reinjected back to the Packet Forwarding Engine for regular forwarding.

When a service set cannot be attached to an interface, use a next-hop service set.

#### Example: Interface Service Set

The following service set can be attached to any media interface of family type **inet**:

```
[edit]
services {
  service-set sset1 {
    extension-service jnx-flow {
      provider-specific rules;
    }
    # Existing hierarchy
    interface-service {
      service-interface { # Indicates service set is an interface service set
      ms-x/y/0.0; # Specifies which PIC to install this policy on
    }
  }
}
```

To associate a defined service set with an interface, include the **service-set** statement at the [**edit interfaces** *interface-name* **unit** *logical-unit-number* **family inet service** (**input** | **output**)] hierarchy level. The following configuration attaches the service set **sset1** to the media interface **ge-0/0/0.0**:

```
[edit]
# Existing hierarchy
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        service {
          input {
            service-set sset1; # Attach service set to input
          }
          output {
            service-set sset1; # Attach service set to output
          }
        }
      }
    }
  }
}
```

#### Example: Next-Hop Service Set

In the following example, the service set sset1 cannot be attached to an interface; instead, two routes are added to direct traffic to the PIC:

```
[edit]
services {
   service-set sset1 {
      extension-service jnx-flow {
         provider-specific rules;
      }
      # Existing hierarchy
      next-hop-service { # Indicates service set is a next-hop service set
         inside-service-interface ms-1/2/0.0;
         outside-service-interface ms-1/2/0.1;
      }
   }
}
```

### *Limitations and Constraints for SDK Services Sets*

The following limits currently apply to service set functionality for the SDK applications:

- You cannot mix JUNOS services and SDK application services in the same service set.
- You cannot run JUNOS services and SDK application services on the same PIC.
- You cannot mix services from SDK applications developed by different providers on the same PIC.
- The inside-service-interface and outside-service-interface logical units cannot be shared across service sets.

## Configuring Traffic Sampling for SDK Applications

This section describes the configuration of traffic sampling for SDK applications. For more information on sampling in the JUNOS software, see the JUNOS configuration guides.

For routing platforms containing a MultiServices PIC, the existing interface statement at the [edit forwarding-options sampling family *family* output] hierarchy level is extended to allow you to use an interface of the ms type (ms-*fpc*/*pic*/*port*) to sample traffic passing through the routing platform. You configure this interface similar to the way you configure traffic sampling for a Monitoring Services or an Adaptive Services PIC.

As with regular JUNOS software, to configure traffic sampling on a PIC, you must complete three tasks: create a firewall filter, apply it to the logical interface on which you want to sample traffic, and enable sampling.

### *Enabling Sampling on a MultiServices PIC*

To enable sampling on a MultiServices PIC, include the input and output statements at the [edit forwarding-options sampling] hierarchy level:

```
[edit]
forwarding-options {
   sampling {
      input {
         family inet {
            rate number;
         }
      }
      output {
         extension-service service-name {
            provider-specific rules;
         }
         interface ms-fpc/pic/port;
      }
   }
}
```

The extension-service statement provides a section of the configuration hierarchy in which the provider of your SDK application may have added its own traffic monitoring configuration statements. To enable sampling for SDK applications and be able to use the configuration statements the SDK application provider may have added, you must include the extension-service statement at the [edit forwarding-options sampling output] hierarchy level. For application-specific configuration guidelines, see the documentation provided with your application.

**NOTE:** If you use the extension-service statement, the only other statement you can include at the [edit forwarding-options sampling output] hierarchy level is the interface statement. In this case, you must set the interface statement to an interface with an ms prefix.

### *Example: Traffic Sampling on a MultiServices PIC*

The following example shows a firewall filter sample-monitor, which, when attached to an interface, ensures that all traffic entering that interface with a source address matching address 10.1.1.1 is sampled and sent to the output interface ms-2/0/0.

```
[edit]
firewall {
   family inet {
      filter sample-monitor {
         term sample-term {
            from {
               source-address {
                  10.1.1.1/32;
               }
            }
            then {
```

```
                sample;
                accept;
            }
        }
    }
}
forwarding-options {
    sampling {
        input {
            family inet {
                rate 1;
            }
        }
        output {
            extension-service abc-sample {
                provider-specific rules;
            }
            interface ms-2/0/0;
        }
    }
```

You can attach the firewall filter created in the above sample to any interface in your network.

### *Limitations and Constraints*

The following are limitations of traffic monitoring as supported for JUNOS SDK applications:

- Traffic monitoring is supported for IPv4 only.
- Firewall filters are used on ingress interfaces to direct packets for sampling or port mirroring. Sampling and port mirroring cannot be enabled on the same traffic.
- Only one extension-service statement can be used.
- Only one interface can be configured for sampling.

## Tracing Process Monitoring Operations

The process health monitor (pmond) is the central monitoring process for SDK applications. It tracks resource usage and performs actions on processes when they trigger certain events (for example, when there is a runaway process event or when low-water or high-water resource marks are exceeded). Process monitoring ensures that SDK applications are operating appropriately and provides an interface for operators to monitor the impact of their SDK applications on the Routing Engine.

To trace process monitoring operations, include the process-monitor statement at the [edit system processes] hierarchy level:

```
[edit]
system {
    processes {
```

```
        process-monitor {
            disable;
            traceoptions {
                file;
                flag flag;
                level level;
                no-remote-trace;
            }
        }
    }
}
```

The traceoptions statement is the only container statement at the [edit system processes process-monitor] hierarchy level. The available flags for the traceoptions statement include:

- all—Enable all traceoptions flags.
- process-tracking—Display process life-cycle events and parent/child pedigree changes.
- heartbeat—Display heartbeat updates from applications.
- ui—Display tracing messages for UI operational commands.

## Tracing System Resource Cleanup Operations

Using the JUNOS SDK, developers can have their SDK applications request and manage system resources. Some of this resource utilization is persistent across, for example, reboots or the restart of the application. And some system tasks such as deleting a package, disabling and application, or accessing shared resources require that resources be cleaned up by entities other than the application itself. Resources that are known to need cleaning up include the following:

- GENCFG blobs
- SYSV shared memory segments
- SYSV semaphores
- Temporary files

Currently, the traceoptions statement is the only CLI statement available for configuring resource cleanup. The traceoptions flag option has several flags for selectively turning the debugging of trace messages on or off:

```
[edit]
system {
    processes {
        resource-cleanup {
            traceoptions {
                flag (all | events | gencfg | sysvsem | sysvshm | ui);
                level level;
            }
        }
    }
```

```
}
```

The available flags for the traceoptions statement include:

- all—Enable all traceoption flags.
- events—Display process state change and cleanup events.
- gencfg—Display GENCFG blobs recorded for cleanup.
- sysvsem—Display SYSV semaphores recorded for cleanup.
- sysvshm—Display SYSV shared memory segments recorded for cleanup.
- ui—Display tracing messages for UI operational commands.

Chapter 20

# Using Configuration Mode Commands with SDK Applications

This material pertains only to configuring routers that run JUNOS SDK applications.

Configuration mode commands are commands you enter in configuration mode that perform general configuration functions such as copying, navigating, and managing configuaration files. The SDK configuration mode commands are described in the following topics.

The following topics describe commands that identify and operate on configuration statements based on the SDK application package that defines them:



## Displaying Additional Information About Installed SDK Application Packages

To determine if a configuration has settings contributed by an SDK application package, use the following configuration mode command:

```
user@host# show <statement-path> | display detail
```

This command displays the configuration schema as piped through to the display detail command. The show command displays the entire user-defined configuration unless it is limited by the optional statement-path variable to that branch of the configuration schema. The display detail command displays the characteristics, descriptions, and constraints of each configuration statement in the JUNOS configuration schema using comment lines.

Generally, the information displayed is help strings and the permission bits required to add or modify the configuration statement. For configuration statements that are defined by an SDK application package, the name of the package that defines the statement. Also, if a JUNOS statement is redefined by an SDK application package, the package name is listed. But if a configuration statement is defined by the native JUNOS software only, no package name is displayed.

### *Example: show jnx-example | display detail Command*

This example compares the output from the show jnx-example and show jnx-example | display detail commands.

**NOTE:** The statement jnx-example in this example is a configuration object added to the configuration schema by the provider of the SDK application package and is not part of the native JUNOS configuration schema. (It happens that the package name is also named jnx-example.)

```
[edit]
user@router# show jnx-example
jnx-example {
    jnx-example-data hello {
        description hello;
    }
}

[edit]
user@router# show jnx-example | display detail
##
## jnx-example: Example service configuration
## require: jnx-example
## package: jnx-example
##
jnx-example {
    ##
    ## Example data identifier
    ## range: 1 .. 127
    ## package: jnx-example
    ##
    jnx-example-data hello {
        ##
        ## description: General description of data
        ## range: 1 .. 127
        ## package: jnx-example
        ##
        description hello;
    }
}
```

## Displaying and Deleting the Configuration for SDK Applications

To display or delete the configuration for a specific SDK application package, use the extension *package-name* (show | delete) configuration mode command:

```
user@host# extension package-name (show | delete) <section>
```

The extension command filters for SDK application configuration statements based on the package named in the extension command starting at the top of the configuration hierarchy, or, if you use the *section* option, starting at the hierarchy level (statement path) specified by *section*.

**NOTE:** Remove all the soon-to-be invalid configurations before removing the SDK application package.

Before removing SDK application packages, use the extension *package-name* show command to display the entire configuration contributed by the named package. Then use the extension *package-name* delete command to remove all configuration statements for that package.

The extension show and extension delete commands select for, or filter, configuration differently, as explained in the following sections.

- Using the extension show Command to Match Package Names on page 661
- Using the extension show Command to Display a Specific Package's Configuration on page 662
- Using the extension delete Command on page 663

### *Using the extension show Command to Match Package Names*

Without the extension *package-name* filter, the show command displays the entire user-defined configuration hierarchy. The extension *package-name* show command, however, displays only the configuration statements contributed by packages whose names match those in the command. The subset of matches includes packages whose package names exactly match the value of *package-name* as well as those whose names have the same root but may have longer names, similar to a wildcard situation. The output displays the settings relating to all matches.

The following example shows simplified output illustrating how the extension show filter works. Suppose a router has packageA, packageB, and packageAB installed. When you issue the show command, you see the following output:

```
user@host# show
system {
   packageA {
      ....
   }
   packageB {
      ....
   }
   packageAB {
      ....
   }
}
```

If you issue the command extension packageA show, you see a subset of the previous show command output. The output displays settings for packages with names that not only exactly match packageA but also have roots that match (in this case, packageAB):

```
user@host# extension packageA show
system {
   packageA {
```

```
        ....
    }
    packageAB {
        ....
    }
}
```

### *Using the extension show Command to Display a Specific Package's Configuration*

The extension *package-name* show command selects configurations contributed by and leading to the named package.

In the following example, only the sdk-backup-server statement at the [edit system radius-server 10.1.1.1] hierarchy level and the sdk-proto1 statement at the [edit system protocols] hierarchy level are contributed by the SDK application package sdk-pkg1:

```
user@host# show
system {
    radius-server {
        10.1.1.1 {
            timeout 10;
            sdk-backup-server 10.1.1.2; # Contributed by sdk-pkg1
        }
    }
}
protocols {
    ospf {
        ....
    }
    sdk-proto1 { # Contributed by sdk-pkg1
        ....
    }
}
```

Following is the output from the extension sdk-pkg1 show command:

```
user@host# extension sdk-pkg1 show
system {
    radius-server {
        10.1.1.1 {
            sdk-backup-server 10.1.1.2;
        }
    }
}
protocols {
    sdk-proto1 {
        ....
    }
}
```

The extension sdk-pkg1 show command filters out the timeout and ospf commands from the displayed output, which were not contributed by the sdk-pkg1 package.

### *Using the extension delete Command*

The extension *package-name* delete command treats the value of *package-name* as a literal. It deletes only the settings contributed by the package whose package name exactly matches the given value. Using this command, you can delete all user-defined configuration statements related to the named package.

**NOTE:** A configuration defined in any native JUNOS package is never deleted by the extension *package-name* delete command.

Continuing with the preceding example, notice how the configuration changes when the extension sdk-pkg1 delete command is used:

```
user@host# extension sdk-pkg1 delete
[edit]
user@host# show
system {
   radius-server {
      10.1.1.1 {
         timeout 10;
      }
   }
}
protocols {
   ospf {
      ....
   }
}
```

You could accomplish the same thing by issuing the following two commands:

- delete system radius-server 10.1.1.1 sdk-backup-server
- delete protocols sdk-proto1

Chapter 21

# Summary of SDK Configuration Mode Commands

The configuration mode commands described in this section are specific to the configuration of SDK applications either in whole or in part. The commands are listed in alphabetical order.

## extension package-name (show | delete)

**Syntax** extension *package-name* (show | delete) <*section*>

**Release Information** Command introduced in JUNOS Release 8.5.

**Description** Manage configurations that are contributed by SDK application packages. Use show to display user-defined configuration contributed by the named package. If you specify delete, all subordinate statements and identifiers contained within the specified statement path (see the *section* option) are deleted as well.

**NOTE:** A configuration defined in any of the native JUNOS packages is never deleted by the extension *package-name* delete command.

**Options** *package-name*—Name of SDK application package.

*section*—(Optional) Statement path from which you want the command to act.

**Required Privilege Level** configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

## show | display detail

**Syntax** show <*hierarchy-level*> | display detail

**Release Information** Command introduced before JUNOS Release 7.4.
package: output field introduced in JUNOS Release 8.5.

**Description** Display additional information about the configuration. The additional information generally includes the help string that explains each configuration statement and the permission bits required to add and modify the configuration statement. If a statement is contributed by an SDK application package, the name of the package is given with the output field ## package: *package-name*.

**Options** *hierarchy-level*—(Optional) Statement hierarchy path for which you want the configuration displayed.

**Required Privilege Level** configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

Chapter 22

# Summary of SDK Configuration Statements

This section provides a reference for each of the SDK configuration statements. The statements are organized alphabetically.

## extension-provider

**Syntax**

```
extension-provider {
    control-cores control-number;
    data-cores data-number;
    forwarding-db-size size;
    object-cache-size size;
    package package-name;
    policy-db-size size;
    wired-process-mem-size size;
    syslog {
        facility severity;
    }
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *slot-number* adaptive-services service-package]

**Release Information** Statement introduced in JUNOS Release 9.0.
object-cache-size option introduced in JUNOS Release 9.1.
forwarding-db-size, syslog, facility, and severity options introduced in JUNOS Release 9.2.
policy-db-size and wired-process-mem-size options introduced in JUNOS Release 9.3.

**Description** Configure an SDK application on a PIC.

**Options**

control-cores *control-number*—Number of cores you want to specify as control cores, which are cores dedicated to run control functionality (application control). At least one core must be a control core.
**Range:** 1 through 8

data-cores *data-number*—Number of cores you want to specify as data cores, which are cores dedicated to processing data for the application (application data).
**Range:** 0 through 7 (recommended minimum is 5).

forwarding-db-size *size*—Size of the forwarding database (FDB) in megabytes (MB).
**Range:** 0 through 1280

object-cache-size *size*—Size of the object cache in MB. Only values in increments of 128 MB are allowed.
**Range:** for MS-100 PIC, 128 through 512. If the PIC is configured with a wired-process-mem-size of 512, the maximum object-cache-size is 128 MB.
**Range:** for MS-400 PIC, 128 through 1280. If the PIC is configured with a wired-process-mem-size of 512, the maximum object-cache-size is 512 MB.

package *package-name*—Name of the SDK application package to be installed on the PIC. There can be up to eight packages installed on a PIC.

policy-db-size *size*—Size of the policy database in MB.
**Range:** Range: 0 through 1280

wired-process-mem-size *size*—Size of the wired process memory in MB.
**Range:** for MS-100 PIC and MS-400 PIC, 0 through 512

The remaining statements are explained separately.

**Usage Guidelines** See "Configuring the MultiServices PIC" on page 648.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## extension-service

**Syntax**
```
extension-service service-name {
    provider-specific rules;
}
```

**Hierarchy Level** [edit services service-set *service-set-name*],
[edit forwarding-options sampling output]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Define an SDK service set or traffic monitoring using application-specific configuration guidelines.

**Options** *provider-specific rules*—Provider-specific subhierarchy for services and service sets. See the application-specific documentation for details.

**Usage Guidelines** See "SDK Applications Configuration Guidelines" on page 647.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

## extensions

**Syntax**
```
extensions {
    providers {
        provider-id;
    }
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Turn on the SDK service process (ssd) and configure the provider ID to enable SDK application packages to be deployed and run on the router.

**Options** providers *provider-id*—Provider ID for the SDK application package. See the application-specific documentation.

**Usage Guidelines** See "Enabling the SDK Service Process and SDK Application Deployment" on page 647.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## process-monitor

**Syntax**

```
process-monitor {
    disable;
    traceoptions {
        file;
        flag flag;
        level level;
        no-remote-trace;
    }
}
```

**Hierarchy Level** [edit system processes]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Configure tracing options for the process health monitor (pmond).

**Options** disable—Disable the health monitor.

The remaining statements are explained separately.

**Usage Guidelines** See “Tracing Process Monitoring Operations” on page 656.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## resource-cleanup

**Syntax**

```
resource-cleanup {
    disable;
    traceoptions {
        file;
        flag flag;
        level level;
        no-remote-trace;
    }
}
```

**Hierarchy Level** [edit system processes]

**Release Information** Statement introduced in JUNOS Release 9.3.

**Description** Selectively turn on or off the debugging of trace messages for the resource cleanup process.

**Options** disable—Disable the resource cleanup process.

The remaining statements are explained separately.

**Usage Guidelines** See "Tracing System Resource Cleanup Operations" on page 657.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

## service-order

**Syntax**

```
service-order {
   forward-flow [ service-name1 service-name2 ];
   reverse-flow [ service-name1 service-name2 ];
}
```

**Hierarchy Level** [edit services service-set *service-set-name*]

**Release Information** Statement introduced in JUNOS Release 9.3.

**Description** Define order of services in service set to be applied to traffic coming to the PIC.

**Options** forward-flow—Order of services in service set to be applied in forward flow.

reverse-flow—Order of services in service set to be applied in reverse flow. If you want the order to be the reverse of that specified for forward flow, this is optional. But if, for example, you want the order to be the same regardless of direction of flow, you need to include this statement.

**Usage Guidelines** See "Configuring SDK Service Sets" on page 650.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** extension-service

## syslog

**Syntax**

```
syslog {
    facility severity;
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *slot-number* adaptive-services service-package extension-provider]

**Release Information** Statement introduced in JUNOS Release 9.2.

**Description** Enable PIC system logging to record or view system log messages on a specific PIC, The system log information is passed to the kernel for logging in the /var/log/messages directory.

**Options** *facility*—Group of messages that are either generated by the same software process or concern a similar condition or activity. Possible values:

- pfe
- external

*severity*—Classification of effect on functioning. Possible values are the same as for the native JUNOS software. For more information about severity, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 115. Possible values include the following:

- any—Include all severity levels.
- none—Disable logging of the associated facility to a destination.
- emergency—System panic or other condition that causes the routing platform to stop functioning.
- alert—Conditions that require immediate correction, such as a corrupted system database.
- critical—Critical conditions, such as hard errors.
- error—Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- warning—Conditions that warrant monitoring.
- notice—Conditions that are not errors but might warrant special handling.
- info—Events or nonerror conditions of interest.

**Usage Guidelines** "Configuring the MultiServices PIC" on page 648.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** extension-provider

## traceoptions

See the following sections:

- traceoptions (Process Monitor) on page 677
- traceoptions (Resource Cleanup) on page 679

## *traceoptions (Process Monitor)*

**Syntax**

```
traceoptions {
    file <filename> <files number> <match regular-expression> <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    level level;
    no-remote-trace;
}
```

**Hierarchy Level** [edit system processes process-monitor]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** Enable tracing options for the process health monitor (pmond).

**Options** file—Specify trace file information. You can include the following options:

- files *number*—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

- match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

- size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches its maximum size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- world-readable | no-world-readable—(Optional). Grant all users permission to read log files, or restrict the permission only to the root user and users who have the JUNOS maintenance permission.

flag *flag*—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- all—Enable all trace options flags.
- events—Trace process state change and cleanup events.
- gencfg—Trace GENCFG blobs recorded for cleanup.
- module—Trace module code.
- sysvsem—Trace SYSV semaphores recorded for cleanup.
- sysvshm—Trace SYSV shared memory segments recorded for cleanup.
- tracking—Trace tracking code.
- ui—Trace user interface operations.

level *level*—Specify the level of debugging output:

- all—Match all levels.
- error—Match error conditions.
- info—Match informational messages.
- notice—Match conditions that warrant special handling (but are not errors).
- verbose—Match verbose messages.
- warning—Match warning messages.

no-remote-trace—Disable remote tracing.

**Usage Guidelines** See "Tracing Process Monitoring Operations" on page 656.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** process-monitor

## *traceoptions (Resource Cleanup)*

**Syntax**

```
traceoptions {
    file <filename> <files number> <match regular-expression> <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    level level;
    no-remote-trace;
}
```

**Hierarchy Level** [edit system processes resource-cleanup]

**Release Information** Statement introduced in JUNOS Release 9.3.

**Description** Enable debugging tracing for resource cleanup process.

**Options** file—Specify trace file information. You can include the following options:

- files *number*—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

- match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

- size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches its maximum size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- world-readable | no-world-readable—(Optional). Grant all users permission to read log files, or restrict the permission only to the root user and users who have the JUNOS maintenance permission.

flag *flag*—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- all—Enable all trace options flags.
- events—Trace process state change and cleanup events.
- gencfg——Trace GENCFG blobs recorded for cleanup.
- module—Trace module code.
- sysvsem—Trace SYSV semaphores recorded for cleanup.
- sysvshm—Trace SYSV shared memory segments recorded for cleanup.
- tracking—Trace tracking code.
- ui—Trace user interface operations.

level *severity*—Specify the level of debugging output:

- all—Match all levels.
- error—Match error conditions.
- info—Match informational messages.
- notice—Match conditions that warrant special handling (but are not errors).
- verbose—Match verbose messages.
- warning—Match warning messages.

no-remote-trace—Disable remote tracing.

**Usage Guidelines** See "Tracing System Resource Cleanup Operations" on page 657.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Topics** resource-cleanup

Chapter 23

# Summary of SDK Operational Commands

Operational mode commands show you the current status of the router interfaces, chassis, protocols, and system information and are used to monitor and troubleshoot configurations.

The operational commands described in this section are relevant to the configuration of SDK applications. For JUNOS operational commands, see the JUNOS command references.

Commands in this section are listed in alphabetical order.

## show chassis pic

**Syntax** show chassis pic fpc-slot *slot-number* pic-slot *slot-number*

**Release Information** Command introduced before JUNOS Release 7.4.

**Description** For PICs with SDK application packages installed, the show chassis pic command displays Extension-provider in the Package field. For more information about this command, see the *JUNOS System Basics and Services Command Reference*.

**Options** See the show chassis pic command in the *JUNOS System Basics and Services Command Reference*.

**Required Privilege Level** view

**List of Sample Output** show chassis pic on page 682

**Output Fields** For a description of the output fields, see the output fields table for the show chassis pic command in the *JUNOS System Basics and Services Command Reference*.

**show chassis pic**

```
user@host> show chassis pic pic-slot 1 fpc-slot 1

FPC slot 1, PIC slot 1 information:
  Type                        MultiServices 100
  State                       Online
  PIC version                 1.5
  Uptime                      5 hours, 59 minutes, 34 seconds
  Package                     Extension-provider
```

## show extension-provider system connections

**Syntax**
show extension-provider system connections
<extensive>
<inet | inet6>
<interface>
<show-routing-instances>

**Release Information**
Command introduced in JUNOS Release 9.1.

**Description**
Show connection activity on the extension provider PIC. This command functions the same as the show system connections command.

**Options**
extensive—(Optional) Display exhaustive system process information.

inet | inet6—(Optional) Display IPv4 connections or IPv6 connections, respectively.

interface—(Optional) Display the name of the extension provider interface.

show-routing-instances—(Optional) Display routing instances.

**Required Privilege Level**
view

**List of Sample Output**


**Output Fields**
For a description of the output fields, see the output fields table for the show system connections command in the *JUNOS System Basics and Services Command Reference*.

**show extension-provider system connections**

```
user@host> show extension-provider system connections
Interface: ms-0/0/0
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  20.0.0.16.32004        20.0.0.1.64292         ESTABLISHED
tcp4       0      0  20.0.0.16.3000         20.0.0.1.58036         ESTABLISHED
tcp4       0      0  20.0.0.16.59517        20.0.0.1.3000          ESTABLISHED
tcp4       0      0  *.3000                 *.*                    LISTEN
tcp4       0      0  *.32004                *.*                    LISTEN
tcp4   66312      0  20.0.0.16.59592        20.0.0.1.32003         ESTABLISHED
tcp4       0      0  *.23                   *.*                    LISTEN
tcp4       0      0  *.33005                *.*                    LISTEN
tcp4       0      0  128.0.1.16.49900       128.0.0.1.6234         ESTABLISHED
udp4       0      0  *.842                  *.*
udp4       0      0  127.0.0.1.123          *.*
udp4       0      0  *.123                  *.*
udp46      0      0  *.514                  *.*
udp4       0      0  *.514                  *.*
Interface: ms-0/2/0
Active Internet connections (including servers)
```

```
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  20.0.0.18.32004        20.0.0.1.62402         ESTABLISHED
tcp4       0      0  *.33005                *.*                    LISTEN
tcp4       0      0  128.0.3.16.59592       128.0.0.1.6234         ESTABLISHED
tcp4       0      0  *.23                   *.*                    LISTEN
tcp4       0      0  *.32004                *.*                    LISTEN
tcp4       0      0  20.0.0.18.49900        20.0.0.1.32003         ESTABLISHED
udp4       0      0  *.789                  *.*
udp4       0      0  127.0.0.1.123          *.*
udp4       0      0  *.123                  *.*
udp46      0      0  *.514                  *.*
udp4       0      0  *.514                  *.*
```

**show extension-provider system connections extensive interface**

```
user@host> show extension-provider system connections extensive interface ms-0/2/0
Interface: ms-0/2/0
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  20.0.0.18.32004        20.0.0.1.49792         ESTABLISHED
   sndsbcc:          0 sndsbmbcnt:          0  sndsbmbmax:     265248
sndsblowat:       2048 sndsbhiwat:      33156
   rcvsbcc:          0 rcvsbmbcnt:          0  rcvsbmbmax:     530496
rcvsblowat:          1 rcvsbhiwat:      66312
   proc id:          1  proc name:
       iss: 4025626166      sndup: 4025626167
    snduna: 4025626167     sndnxt: 4025626167      sndwnd:      66312
    sndmax: 4025626167    sndcwnd:     131070 sndssthresh: 1073725440
       irs: 3544420903      rcvup: 3544420904
    rcvnxt: 3544421176     rcvadv: 3544487488      rcvwnd:      66312
       rtt:          0       srtt:         64        rttv:         16
    rxtcur:       1200   rxtshift:          0       rtseq:          0
    rttmin:       1000  mss:       1228
     flags: REQ_SCALE RCVD_SCALE REQ_TSTMP RCVD_TSTMP SACK_PERMIT [0x20003e0]
...
```

**show extension-provider system connections inet**

The output for the show extension-provider system connections inet command is identical to that for the show extension-provider system connections command. For sample output, see show extension-provider system connections on page 683.

**show extension-provider system connections inet6**

```
user@host> show extension-provider system connections inet6
Interface: ms-0/0/0
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
udp6       0      0  *.123                  *.*
udp46      0      0  *.514                  *.*
Interface: ms-0/2/0
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
udp6       0      0  *.123                  *.*
udp46      0      0  *.514                  *.*
```

**show extension-provider system connections interface**

```
user@host> show extension-provider system connections interface ms-0/2/0
Interface: ms-0/2/0
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  20.0.0.18.32004        20.0.0.1.59521         ESTABLISHED
tcp4       0      0  *.33005                *.*                    LISTEN
tcp4       0      0  128.0.3.16.51534       128.0.0.1.6234         ESTABLISHED
tcp4       0      0  *.23                   *.*                    LISTEN
```

```
tcp4       0      0  *.32004                *.*                    LISTEN
tcp4       0      0  20.0.0.18.61044        20.0.0.1.32003         ESTABLISHED
udp4       0      0  *.914                  *.*
udp4       0      0  127.0.0.1.123          *.*
udp4       0      0  *.123                  *.*
udp46      0      0  *.514                  *.*
udp4       0      0  *.514                  *.*
```

**show extension-provider system connections show-routing-instances**

```
user@host> show extension-provider system connections show-routing-instances

Interface: ms-0/0/0
Active Internet connections (including servers) (including routing-instances)
Proto Recv-Q Send-Q Local Address Foreign Address Routing Instance  (state)
tcp4     0   0 20.0.0.16.32004  20.0.0.1.52590 __juniper_private2__ ESTABLISHED
tcp4     0   0 20.0.0.16.3000   20.0.0.1.58036 __juniper_private2__ ESTABLISHED
tcp4     0   0 20.0.0.16.59517  20.0.0.1.3000  __juniper_private2__ ESTABLISHED
tcp4     0   0 *.3000           *.*            __juniper_private2__ LISTEN
tcp4     0   0 *.32004          *.*            __juniper_private2__ LISTEN
tcp4 66312   0 20.0.0.16.59592  20.0.0.1.32003 __juniper_private2__ ESTABLISHED
tcp4     0   0 *.23             *.*            __juniper_private1__ LISTEN
tcp4     0   0 *.33005          *.*            __juniper_private2__ LISTEN
tcp4     0   0 128.0.1.16.49900 128.0.0.1.6234 __juniper_private1__ ESTABLISHED
udp4     0   0 *.842            *.*            __juniper_private1__
udp4     0   0 127.0.0.1.123    *.*            default
udp4     0   0 *.123            *.*            __juniper_private1__
udp46    0   0 *.514            *.*            default
udp4     0   0 *.514            *.*            __juniper_private1__
Interface: ms-0/2/0
Active Internet connections (including servers) (including routing-instances)
Proto Recv-Q Send-Q Local Address Foreign Address Routing Instance  (state)
tcp4     0   0 20.0.0.18.32004  20.0.0.1.54602 __juniper_private2__ ESTABLISHED
tcp4     0   0 *.33005          *.*            __juniper_private2__ LISTEN
tcp4     0   0 128.0.3.16.59592 128.0.0.1.6234 __juniper_private1__ ESTABLISHED
tcp4     0   0 *.23             *.*            __juniper_private1__ LISTEN
tcp4     0   0 *.32004          *.*            __juniper_private2__ LISTEN
tcp4     0   0 20.0.0.18.49900  20.0.0.1.32003 __juniper_private2__ ESTABLISHED
udp4     0   0 *.789            *.*            __juniper_private1__
udp4     0   0 127.0.0.1.123    *.*            default
udp4     0   0 *.123            *.*            __juniper_private1__
udp46    0   0 *.514            *.*            default
udp4     0   0 *.514            *.*            __juniper_private1__
```

**show extension-provider system connections show-routing-instances interface inet6**

```
user@host> show extension-provider system connections show-routing-instances
interface ms-0/0/0 inet6

Interface: ms-0/0/0
Active Internet connections (including servers) (including routing-instances)
Proto Recv-Q Send-Q  Local Address         Foreign Address       Routing Instance
       (state)
udp6       0      0  *.123                  *.*                    default
udp46      0      0  *.514                  *.*                    default
```

## show extension-provider system packages

**Syntax**
show extension-provider system packages
<detail>
<interface>

**Release Information**
Command introduced in JUNOS Release 9.1.

**Description**
Show packages loaded on the extension provider PIC. This command functions the same as the show system software command.

**Options**
none—TBD

detail—(Optional) Display detailed output.

interface—(Optional) Display the name of the extension provider interface.

**Required Privilege Level**
view

**List of Sample Output**
show extension-provider system packages on page 686
show extension-provider system packages detail on page 686
show extension-provider system packages interface on page 687

**Output Fields**
Output field descriptions to be provided.

**show extension-provider system packages**

```
user@host> show extension-provider system packages
Interface: ms-0/0/0
jmpsdk              JUNOS MPSDK Base OS boot [9.2R1.3]
jnx-flow-data-pic   JUNOS SDK JNX-FLOW Dataplane Component [9.2I20080801_1059]
Interface: ms-0/2/0
jmpsdk              JUNOS MPSDK Base OS boot [9.2R1.3]
```

**show extension-provider system packages detail**

```
user@host> show extension-provider system packages detail
Interface: ms-0/0/0
Information for jmpsdk:
Comment:
JUNOS MPSDK Base OS boot [9.2R1.3]
Description:
JUNOS MPSDK Base OS
Copyright (c) 1996-2008, Juniper Networks, Inc.
All rights reserved.
Software version:       9.2R1.3
This package contains the MPSDK base operating system components.
Information for jnx-flow-data-pic:
Comment:
JUNOS SDK JNX-FLOW Dataplane Component [9.2I20080801_1059]
Description:
JUNOS SDK JNX-FLOW Data Component Package
Copyright (c) 1996-2008, Juniper Networks, Inc.
All rights reserved.
Software version:       9.2I20080801_1059
This package contains SDK JNX-FLOW dataplane component
Interface: ms-0/2/0
Information for jmpsdk:
Comment:
JUNOS MPSDK Base OS boot [9.2R1.3]
```

```
Description:
JUNOS MPSDK Base OS
Copyright (c) 1996-2008, Juniper Networks, Inc.
All rights reserved.
Software version:       9.2R1.3
This package contains the MPSDK base operating system components.
```

**show extension-provider system packages interface**

```
user@host> show extension-provider system packages interface ms-0/2/0
Interface: ms-0/2/0
jmpsdk              JUNOS MPSDK Base OS boot [9.2R1.3]
```

## show extension-provider system processes

**Syntax** show extension-provider system processes
<brief | detail | extensive>
<interface>
<wide>

**Release Information** Command introduced in JUNOS Release 9.1.

**Description** Show system process table on the extension provider PIC.

**Options** brief | detail | extensive—(Optional) Display the specified level of output.

interface—(Optional) Name of the extension provider interface.

wide—(Optional) Display information even if it is wider than 80 columns.

**Required Privilege Level** view

**List of Sample Output**


**Output Fields** For a description of the output fields, see the output fields table for the show system processes command in the *JUNOS System Basics and Services Command Reference*.

**show extension-provider system processes**

```
user@host> show extension-provider system processes

Interface: ms-0/0/0
  PID  TT  STAT      TIME COMMAND
    0  ??  WLs    0:00.00 [swapper]
    1  ??  SLs    0:00.75 /sbin/init --
    2  ??  DL     0:05.91 [g_event]
    3  ??  DL     0:03.96 [g_up]
    4  ??  DL     0:04.24 [g_down]
    5  ??  DL     0:00.00 [kqueue taskq]
    6  ??  DL     0:00.00 [thread taskq]
    9  ??  DL     0:00.15 [pagedaemon]
   10  ??  DL     0:00.00 [ktrace]
   11  ??  RL     0:00.00 [idle: cpu31]
   12  ??  RL     0:00.00 [idle: cpu30]
   13  ??  RL     0:00.00 [idle: cpu29]
   14  ??  RL     0:00.13 [idle: cpu28]
   15  ??  RL     0:00.00 [idle: cpu27]
   16  ??  RL     0:00.00 [idle: cpu26]
   17  ??  RL     0:00.00 [idle: cpu25]
   18  ??  RL     0:00.13 [idle: cpu24]
   19  ??  RL     0:00.00 [idle: cpu23]
   20  ??  RL     0:00.00 [idle: cpu22]
   21  ??  RL     0:00.00 [idle: cpu21]
   22  ??  RL     0:00.13 [idle: cpu20]
   23  ??  RL     0:00.00 [idle: cpu19]
   24  ??  RL     0:00.00 [idle: cpu18]
```

```
   25  ??  RL     0:00.00 [idle: cpu17]
   26  ??  RL     0:00.13 [idle: cpu16]
   27  ??  RL     0:00.00 [idle: cpu15]
   28  ??  RL     0:00.00 [idle: cpu14]
   29  ??  RL     0:29.15 [idle: cpu13]
   30  ??  RL   443:15.66 [idle: cpu12]
   31  ??  RL     0:29.15 [idle: cpu11]
   32  ??  RL     0:29.14 [idle: cpu10]
. . .
```

**show extension-provider system processes brief**

```
user@host> show extension-provider system processes brief
Interface: ms-0/0/0
last pid: 20238;  load averages: 11.64, 11.71, 11.74  up 0+07:24:28    22:23:18
91 processes:  45 running, 34 sleeping, 12 waiting
Mem: 8924K Active, 1768K Inact, 152M Wired, 156K Cache, 77M Buf, 200M Free
Swap:
Interface: ms-0/2/0
last pid: 13025;  load averages:  4.16,  4.08,  4.02  up 0+04:43:20    22:23:18
88 processes:  37 running, 32 sleeping, 19 waiting
Mem: 6488K Active, 1212K Inact, 156M Wired, 24K Cache, 75M Buf, 460M Free
Swap:
```

**show extension-provider system processes detail**

```
user@host> show extension-provider system processes detail
Interface: ms-0/0/0
  PID   UID  PPID CPU PRI NI   RSS WCHAN  STARTED  TT  STAT      TIME COMMAND
   20     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   21     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   22     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.13 [idle: cp
   28     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   15     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   19     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   11     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   12     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   13     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   16     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   17     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   18     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.13 [idle: cp
   26     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.13 [idle: cp
   68     0     0   0 -16  0     8 -       2:59PM  ??  RL     0:00.00 [pot: cpu
   70     0     0   0 -16  0     8 -       2:59PM  ??  RL     0:00.00 [poller:
   14     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.13 [idle: cp
   24     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   25     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   27     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   69     0     0   0 -16  0     8 -       2:59PM  ??  RL     0:00.00 [poller:
   23     0     0   0 171  0     8 -       2:59PM  ??  RL     0:00.00 [idle: cp
   30     0     0   0 171  0     8 -       2:59PM  ??  RL   444:58.30 [idle: cp
  259     0     1   0 139  0   840 -       2:59PM  ??  R    3111:46.43 /opt/sdk/

  120     0     1   0 139  0   652 select  2:59PM  ??  Ss   154:48.02 syslogd -
  142     0     1   0   8  0  1132 wait    2:59PM  ??  S    122:57.26 /usr/sbin
20287     0   142   0 109  0  1100 -      10:24PM  ??  R      0:00.08 /bin/ps -
    0     0     0   0 -16  0     0 -       2:59PM  ??  WLs    0:00.00 [swapper]
    1     0     0   0   8  0  1152 wait    2:59PM  ??  SLs    0:00.75 /sbin/ini
. . .
```

**show extension-provider system processes extensive**

```
user@host> show extension-provider system processes extensive
Interface: ms-0/0/0
last pid: 20384;  load averages: 11.51, 11.63, 11.69  up 0+07:27:42    22:26:32
91 processes:  45 running, 34 sleeping, 12 waiting
Mem: 8924K Active, 1784K Inact, 152M Wired, 156K Cache, 77M Buf, 200M Free
Swap:
  PID USERNAME  THR PRI NICE   SIZE    RES STATE  C   TIME   WCPU COMMAND
  259 root        8 139    0   643M   840K CPU13  d  52.1H 658.40% jnx-flow-data

   22 root        1 171   52     0K     8K CPU20  14   0:00 99.22% idle: cpu20
   21 root        1 171   52     0K     8K CPU21  0   0:00 99.22% idle: cpu21
   20 root        1 171   52     0K     8K CPU22  0   0:00 99.22% idle: cpu22
   15 root        1 171   52     0K     8K CPU27  0   0:00 98.49% idle: cpu27
   19 root        1 171   52     0K     8K CPU23  0   0:00 97.71% idle: cpu23
   28 root        1 171   52     0K     8K CPU14  0   0:00 97.71% idle: cpu14
   18 root        1 171   52     0K     8K CPU24  18   0:00 96.97% idle: cpu24
   26 root        1 171   52     0K     8K CPU16  10   0:00 96.97% idle: cpu16
   70 root        1 -16    0     0K     8K CPU8   0   0:00 96.97% poller: cpu8
   68 root        1 -16    0     0K     8K CPU1   0   0:00 96.97% pot: cpu1
   25 root        1 171   52     0K     8K CPU17  0   0:00 96.97% idle: cpu17
   17 root        1 171   52     0K     8K CPU25  0   0:00 96.97% idle: cpu25
   13 root        1 171   52     0K     8K CPU29  0   0:00 96.97% idle: cpu29
   12 root        1 171   52     0K     8K CPU30  0   0:00 96.97% idle: cpu30
   11 root        1 171   52     0K     8K CPU31  0   0:00 96.97% idle: cpu31
   16 root        1 171   52     0K     8K CPU26  0   0:00 96.97% idle: cpu26
   14 root        1 171   52     0K     8K CPU28  1c   0:00 96.24% idle: cpu28
Interface: ms-0/2/0
last pid: 13175;  load averages:  4.00,  4.04,  4.00  up 0+04:46:34    22:26:32
88 processes:  37 running, 32 sleeping, 19 waiting
Mem: 6488K Active, 1228K Inact, 156M Wired, 24K Cache, 75M Buf, 460M Free
Swap:
  PID USERNAME  THR PRI NICE   SIZE    RES STATE  C   TIME   WCPU COMMAND
   12 root        1 171   52     0K     8K CPU30  0   0:00 98.49% idle: cpu30
   23 root        1 171   52     0K     8K CPU19  0   0:00 98.49% idle: cpu19
   20 root        1 171   52     0K     8K CPU22  0   0:00 98.49% idle: cpu22
   21 root        1 171   52     0K     8K CPU21  0   0:00 98.49% idle: cpu21
   75 root        1 -16    0     0K     8K CPU16  4   0:00 97.71% poller: cpu16
   76 root        1 -16    0     0K     8K CPU20  4   0:00 97.71% poller: cpu20
   13 root        1 171   52     0K     8K CPU29  0   0:00 97.71% idle: cpu29
   14 root        1 171   52     0K     8K CPU28  1c   0:00 96.24% idle: cpu28
   77 root        1 -16    0     0K     8K CPU24  4   0:00 96.24% poller: cpu24
   16 root        1 171   52     0K     8K CPU26  0   0:00 96.24% idle: cpu26
   11 root        1 171   52     0K     8K CPU31  0   0:00 96.24% idle: cpu31
   24 root        1 171   52     0K     8K CPU18  0   0:00 96.24% idle: cpu18
   25 root        1 171   52     0K     8K CPU17  0   0:00 96.24% idle: cpu17
   17 root        1 171   52     0K     8K CPU25  0   0:00 96.24% idle: cpu25
   19 root        1 171   52     0K     8K CPU23  0   0:00 96.24% idle: cpu23
   29 root        1 171   52     0K     8K CPU13  d 284:04 93.95% idle: cpu13
   30 root        1 171   52     0K     8K CPU12  c 284:05 92.48% idle: cpu12
   33 root        1 171   52     0K     8K CPU9   9 283:52 92.48% idle: cpu9
```

**show extension-provider system processes interface**

The output for the show extension-provider system processes interface command is identical to that for the show extension-provider system processes command except that the output for the former is for the specified interface only and the output for the latter is for all ms interfaces. For sample output, see show extension-provider system processes on page 688.

**show extension-provider system processes wide**

```
user@host> show extension-provider system processes wide

Interface: ms-1/0/0
  PID  TT  STAT      TIME PROVIDER COMMAND
    0  ??  WLs    0:00.00 (null)   [swapper]
    1  ??  SLs    0:00.83          /sbin/init --
    2  ??  DL     0:24.86          [g_event]
    3  ??  DL     0:24.52          [g_up]
    4  ??  DL     0:24.38          [g_down]
    5  ??  DL     0:00.00          [thread taskq]
    6  ??  DL     0:00.00          [kqueue taskq]
    9  ??  DL     0:00.53          [pagedaemon]
   10  ??  DL     0:00.00          [ktrace]
   11  ??  RL     0:00.00          [idle: cpu31]
   12  ??  RL     0:00.00          [idle: cpu30]
   13  ??  RL     0:00.00          [idle: cpu29]
   14  ??  RL     0:00.17          [idle: cpu28]
   15  ??  RL     0:00.00          [idle: cpu27]
   16  ??  RL     0:00.00          [idle: cpu26]
   17  ??  RL     0:00.00          [idle: cpu25]
   18  ??  RL     0:00.17          [idle: cpu24]
   19  ??  RL     0:00.00          [idle: cpu23]
   20  ??  RL     0:00.00          [idle: cpu22]
   21  ??  RL     0:00.00          [idle: cpu21]
   22  ??  RL     0:00.17          [idle: cpu20]
   23  ??  RL     0:00.00          [idle: cpu19]
   24  ??  RL     0:00.00          [idle: cpu18]
   25  ??  RL     0:00.00          [idle: cpu17]
   26  ??  RL     0:00.17          [idle: cpu16]
   ...
```

**show extension-provider system processes wide detail**

```
user@host> show extension-provider system processes wide detail

Interface: ms-0/2/0
PID UID PPID CPU PRI NI RSS WCHAN STARTED TT STAT TIME COMMAND    PROVIDER
 12   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu30]
 20   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu22]
 23   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu19]
 21   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu21]
 25   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu17]
 11   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu31]
 13   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu29]
 14   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.36 [idle: cpu28]
 16   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu26]
 17   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu25]
 19   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu23]
 24   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu18]
 75   0    0   0 -16  0   8 -   5:40PM ?? RL   0:00.00 [poller: cpu16]
 76   0    0   0 -16  0   8 -   5:40PM ?? RL   0:00.00 [poller: cpu20]
 77   0    0   0 -16  0   8 -   5:40PM ?? RL   0:00.00 [poller: cpu24]
 29   0    0   0 171  0   8 -   5:40PM ?? RL 288:22.84 [idle: cpu13]
 15   0    0   0 171  0   8 -   5:40PM ?? RL   0:00.00 [idle: cpu27]
 74   0    0   0 -16  0   8 -   5:40PM ?? RL   0:00.00 [pot: cpu1]
 33   0    0   0 171  0   8 -   5:40PM ?? RL 288:47.94 [idle: cpu9]
 30   0    0   0 171  0   8 -   5:40PM ?? RL 287:07.79 [idle: cpu12]
 34   0    0   0 171  0   8 -   5:40PM ?? RL 288:57.04 [idle: cpu8]
 37   0    0   0 171  0   8 -   5:40PM ?? RL 288:01.05 [idle: cpu5]
 38   0    0   0 171  0   8 -   5:40PM ?? RL 285:08.89 [idle: cpu4]
 42   0    0   0 171  0   8 -   5:40PM ?? RL 281:47.55 [idle: cpu0]
  0   0    0   0 -16  0   0 -   5:40PM ?? WLs  0:00.00 [swapper]    null)
```

```
  1  0   0   0   8  0 1144 wait 5:40PM ?? SLs  0:00.58 /sbin/init –
...
```

## show extension-provider system uptime

**Syntax** show extension-provider system uptime
<interface>

**Release Information** Command introduced in JUNOS Release 9.1.

**Description** Show uptime on the extension provider PIC.

**Options** interface—(Optional) Name of the extension provider interface.

**Required Privilege Level** view

**List of Sample Output** show extension-provider system uptime on page 693
show extension-provider system uptime interface on page 693

**Output Fields** For a description of the output fields, see the output fields table for the show system uptime command in the *JUNOS System Basics and Services Command Reference*.

**show extension-provider system uptime**

```
user@host> show extension-provider system uptime
Interface: ms-0/0/0
 5:08PM  up 26 mins, 0 users, load averages: 0.09, 0.06, 0.04
Interface: ms-0/2/0
 5:08PM  up 26 mins, 0 users, load averages: 0.15, 0.03, 0.01
```

**show extension-provider system uptime interface**

```
user@host> show extension-provider system uptime interface ms-0/2/0
Interface: ms-0/2/0
 5:08PM  up 26 mins, 0 users, load averages: 0.15, 0.03, 0.01
```

## show extension-provider system virtual-memory

**Syntax** show extension-provider system virtual-memory
<interface>

**Release Information** Command introduced in JUNOS Release 9.1.

**Description** Show kernel dynamic memory usage on the extension provider PIC. Display the usage of JUNOS kernel memory listed first by size of allocation and then by type of usage.

**Options** interface—(Optional) Name of the extension provider interface.

**Required Privilege Level** view

**List of Sample Output** show extension-provider system virtual-memory on page 694
show extension-provider system virtual-memory interface on page 695

**Output Fields** For a description of the output fields, see Table 40 on page 694. Output fields are listed in the approximate order in which they appear.

**Table 40: show extension-provider system virtual-memory Output Fields**

| Field | Field Description |
|---|---|
| Interface | Interface ID. |
| Size (unlabeled) | Size of memory block in bytes. |
| Type(s) (unlabeled) | Kernel modules that are using the memory blocks. For a definition of each type, see a FreeBSD book. |
| interrupt | Type of interrupt.<br>■ total—Total number of interrupts for each type.<br>■ rate—Interrupt rate. |
| Total | Total of all interrupts. |

**show extension-provider system virtual-memory**

```
user@host> show extension-provider system virtual-memory
Interface: ms-0/0/0
   916976 cpu context switches
193097320 device interrupts
    43468 software interrupts
        0 traps
   199882 system calls
       78 kernel threads created
     2416  fork() calls
        0 vfork() calls
        0 rfork() calls
        0 swap pager pageins
        0 swap pager pages paged in
        0 swap pager pageouts
```

```
        0 swap pager pages paged out
     1307 vnode pager pageins
     1307 vnode pager pages paged in
        0 vnode pager pageouts
        0 vnode pager pages paged out
        0 page daemon wakeups
        0 pages examined by the page daemon
      454 pages reactivated
    54109 copy-on-write faults
       11 copy-on-write optimized faults
    65858 zero fill pages zeroed
    65190 zero fill pages prezeroed
       10 intransit blocking page faults
   206484 total VM faults taken
        0 pages affected by kernel thread creation
   102942 pages affected by  fork()
        0 pages affected by vfork()
        0 pages affected by rfork()
   144325 pages freed
        0 pages freed by daemon
   102373 pages freed by exiting processes
     1749 pages active
      317 pages inactive
       28 pages in VM cache
    38743 pages wired down
    51895 pages free
     4096 bytes per page
        0 swap pages used
        0 peak swap pages used
   109540 total name lookups
          cache hits (86% pos + 12% neg) system 0% per-directory
          deletions 0%, falsehits 0%, toolong 0%
interrupt               total       rate
clock                177515903      59689
Total                177515903      59689
```

**show extension-provider system virtual-memory interface**

```
user@host> show extension-provider system virtual-memory interface ms-0/2/0
Interface: ms-0/2/0
  6971866 cpu context switches
757808764 device interrupts
   101858 software interrupts
        0 traps
  1129382 system calls
       80 kernel threads created
    15764  fork() calls
        0 vfork() calls
        0 rfork() calls
        0 swap pager pageins
        0 swap pager pages paged in
        0 swap pager pageouts
        0 swap pager pages paged out
     1212 vnode pager pageins
     1212 vnode pager pages paged in
        0 vnode pager pageouts
        0 vnode pager pages paged out
        0 page daemon wakeups
        0 pages examined by the page daemon
      420 pages reactivated
   354621 copy-on-write faults
        0 copy-on-write optimized faults
   430183 zero fill pages zeroed
```

```
   424776 zero fill pages prezeroed
     1434 intransit blocking page faults
  1332189 total VM faults taken
        0 pages affected by kernel thread creation
   648103 pages affected by  fork()
        0 pages affected by vfork()
        0 pages affected by rfork()
   892030 pages freed
        0 pages freed by daemon
   673820 pages freed by exiting processes
     1604 pages active
      309 pages inactive
        6 pages in VM cache
    39994 pages wired down
   117802 pages free
     4096 bytes per page
        0 swap pages used
        0 peak swap pages used
   702497 total name lookups
          cache hits (86% pos + 13% neg) system 0% per-directory
          deletions 0%, falsehits 0%, toolong 0%
interrupt                total       rate
clock                987886798      47811
Total                987886798      47811
```

## show system processes

**Syntax**
show system processes
<wide>

**Release Information**
Command introduced in JUNOS Release 7.4.
PROVIDER column introduced in wide option in JUNOS Release 9.0.

**Description**
Display information about software processes that are running on the router.

**Options**
wide—(Optional) Display process information that might be wider than 80 columns. This option shows the PROVIDER column.

**Required Privilege Level**
view

**List of Sample Output**
show system processes on page 697
show system processes wide on page 697

**Output Fields**
For a description of the output fields, see the output fields table for the show system processes command in the *JUNOS System Basics and Services Command Reference*.

**show system processes**

```
user@host> show system processes
     PID  TT  STAT      TIME COMMAND
   ...
       9  ??  DL     0:00.01 [pagedaemon]
   ...
    6463  ??  DL     0:00.18 [md9]
    6738  ??  S      0:00.44 /usr/sbin/mgd -N
    7001  ??  S      0:00.12 /opt/sbin/jnx-exampled -N
    7063  ??  Ss     0:00.03 mgd: (mgd) (regress)/dev/ttyp0 (mgd)
```

**show system processes wide**

```
user@host> show system processes wide
     PID  TT  STAT      TIME PROVIDER COMMAND
   ...
       9  ??  DL     0:00.01          [pagedaemon]
   ...
    6463  ??  DL     0:00.18          [md9]
    6738  ??  S      0:00.44          /usr/sbin/mgd -N
    7001  ??  S      0:00.12 jnx      /opt/sbin/jnx-exampled -N
    7063  ??  Ss     0:00.03          mgd: (mgd) (regress)/dev/ttyp0 (mgd)
```

## show system processes health

**Syntax** show system process health
<process-name *name* | pid *pid*>

**Release Information** Command introduced in JUNOS Release 8.5.

**Description** Display the resource utilization (health), of all the SDK applications currently running. You can display health information about one specific process by specifying either the process name or the process ID (PID).

**Options** process-name *name*—(Optional) Display health information about the process identified by the process name.

pid *pid*—(Optional) Display health information about the process identified by the PID.

**Required Privilege Level** view

**List of Sample Output**
show system processes health on page 699
show system processes health pid on page 699
show system processes health process-name on page 700

**Output Fields** For a description of the output fields, see Table 41 on page 698. Output fields are listed in the approximate order in which they appear.

**Table 41: show system processes health Output Fields**

| Field Name | Field Description |
|---|---|
| PID | Process ID, a number that identifies the process. |
| Provider | Provider prefix. A string that identifies the provider of the SDK application. |
| Parent process | Process ID of the process that spawned the process in question. |
| Child processes | Process ID of the process that is launched from the process in question:<br>■ Process ID for child process—A number that identifies the child process.<br>■ Name of child process—A string that identifies the child process. |
| CPU accumulated | Maximum amount of CPU time that can be accumulated. |
| Heartbeat | A regular signal sent from a router to indicate that the router is up and running:<br>■ Interval—Number of seconds between heartbeats.<br>■ Allowed misses—Number of missed heartbeats allowed before the application restarts.<br>■ Last seen—Time in seconds when the last heartbeat occurred.<br>■ Total misses—Number of heartbeats missed so far. |

**Table 41: show system processes health Output Fields** *(continued)*

| Field Name | Field Description |
|---|---|
| Resource utilization | How memory is divided:<br>■ Area—Segment of memory.<br>■ Current—Current size of memory segment.<br>■ Max. allowed—Maximum size allowed for memory segment.<br>■ data size—Current and maximum sizes of data segment.<br>■ open files—Number of currently open files and the maximum allowed.<br>■ resident set size—Current and maximum sizes of resident set segment.<br>■ shared memory size—The amount of shared memory the process is using.<br>■ stack size—Current and maximum sizes of stack segment. |

**show system processes health**

```
user@host> show system processes health
PID: 10075 (jnx-flow-mgmt)
Provider: jnx
Parent process: 1 (init)
CPU accumulated: 0 seconds
Resource utilization:
  Area                 Current  Max. allowed
  data size                7KB          32MB
  open files                20            64
  resident set size       12KB          24MB
  shared memory size       4KB
  stack size               2KB           8MB
PID: 420 (jnx-exampled)
 Provider: jnx
 Parent process: 1 (init)
 Child processes: 1
   PID    Process name
   421   jnx-exampled
CPU accumulated: 21 seconds
Heartbeat:
   Interval:       1s
   Allowed misses: 5
   Last seen:      1s ago (0 missed)
   Total misses:   2
Resource utilization:
  Area                 Current  Max. allowed
  data size               24KB          16MB
  open files              23           128
  resident set size     1532KB          24MB
  shared memory size      43KB
  stack size               8KB           8MB
```

**show system processes health pid**

The output for the show system processes health pid *pid* command is identical to that for the show system processes health command except that health information is displayed for only the process specified by the PID. For sample output, see show system processes health on page 699.

**show system processes health process-name**

The output for the show system processes health *process-name* name command is identical to that for the show system processes health command except that health information is displayed for only the process named. For sample output, see show system processes health on page 699.

## show system processes providers

**Syntax** show system processes providers

**Release Information** Command introduced in JUNOS Release 8.5.

**Description** Display information about software processes that are running on the router. The output is similar to that of the show system processes extensive command, but this command displays only provider processes (that is, only external processes). Also, this command output has an extra column labeled PROVIDER to display the provider prefix.

**Required Privilege Level** view

**List of Sample Output** show system processes providers on page 701

**Output Fields** For a description of the output fields, see the output fields table for the show system processes command in the *JUNOS System Basics and Services Command Reference*. This table explains all the fields except for PROVIDER which is for the string that is the provider prefix for the SDK application running the process.

**show system processes providers**

```
user@host> show system processes providers
last pid:  7014;  load averages:  0.19,  0.09,  0.05  up 0+00:57:29    12:54:45
   54 processes:  1 running, 53 sleeping
   Mem: 101M Active, 105M Inact, 31M Wired, 132M Cache, 69M Buf, 369M Free
   Swap: 1536M Total, 1536M Free
     PID USERNAME PROVIDER PRI NICE   SIZE    RES STATE    TIME   WCPU COMMAND
    7001 root     jnx       96    0  3240K  2700K select   0:00  0.00% jnx-exampled
```

## show system resource-cleanup processes

**Syntax** show system resource-cleanup processes <detail>

**Release Information** Command introduced in JUNOS Release 9.3.

**Description** Display the list of processes that have been registered for resource clean up services.

**Options** detail—(Optional) Display the list of processes that have been registered for resource clean up services, along with the resources that have been requested for clean up.

**Required Privilege Level** view

**List of Sample Output** show system resource-cleanup processes on page 702
show system resource-cleanup processes detail on page 702

**Output Fields** For a description of the output fields, see Table 42 on page 702. Output fields are listed in the approximate order in which they appear.

**Table 42: show system resource-cleanup processes Output Fields**

| Field Name | Field Description |
|---|---|
| PID | Process ID, a number that identifes a process. |
| Process name | String that identifies the process. |
| Resources to clean | Resources that have been registered to be cleaned up. |

**show system resource-cleanup processes**

```
user@host> show system resource-cleanup processes
PID     Process name          Resources to clean
420     jnx-exampled          GENCFG, SYSV shared memory
```

**show system resource-cleanup processes detail**

```
user@host> show system resource-cleanup processes detail
PID     Process name          Resources to clean
420     jnx-exampled          GENCFG blob major ID 0x8000, minor ID 0x0000
                              SYSV shared memory ID 65536, key 1108955839
                              SYSV shared memory ID 65537, key 1108955837
```

## show version

**Syntax** show version

**Release Information** Command introduced in JUNOS Release 8.5.

**Description** Display the hostname and version information of the software running on the router. For routers that have SDK application packages installed, the show version command lists those packages.

**Required Privilege Level** view

**List of Sample Output** show version on page 703

**Output Fields** For a description of the output fields, see Table 43 on page 703. Output fields are listed in the approximate order in which they appear.

**Table 43: show version Output Fields**

| Field Name | Field Description |
|---|---|
| Hostname | Router name. |
| Model | Router model number. |
| listing | Package contents installed. |

**show version**

```
user@host> show version
Hostname: router1
Model: m10i
JUNOS Base OS boot [I20070611_2103]
JUNOS Base OS Software Suite [8.5I20070611_2103]
JUNOS Kernel Software Suite [8.5I20070611_2103]
JUNOS Crypto Software Suite [8.5I20070611_2103]
JUNOS Packet Forwarding Engine Support (M/T Common) [8.5I20070611_2103]
JUNOS Packet Forwarding Engine Support (M7i/M10i) [8.5I20070611_2103]
JUNOS Online Documentation [8.5I20070611_2103]
JUNOS Routing Software Suite [8.5I20070611_2103]
JUNOS SDK Gateway Example Control Component [8.5I20070612_1932]
JUNOS SDK Gateway Example Dataplane Component [8.5I20070612_1932]
JUNOS SDK Gateway Example Management Component [8.5I20070612_1932]
```

# Part 6
# Router Chassis

Chapter 24

# Router Chassis Configuration Guidelines

You can configure properties of the router chassis, including conditions that activate the red and yellow alarm LEDs on the router craft interface and SONET/SDH framing and concatenation properties for individual Physical Interface Cards (PICs).

To configure router chassis properties, include the following statements at the [edit chassis] hierarchy level:

**NOTE:** Statements at the [edit chassis redundancy] hierarchy level are described in the *JUNOS High Availability Configuration Guide*.

```
chassis {
    aggregated-devices {
        ethernet {
            device-count number;
            lacp {
                system-priority;
                link-protection;
            }
        }
        sonet {
            device-count number;
        }
    }
    alarm {
        interface-type {
            alarm-name (red | yellow | ignore);
        }
    }
    config-button {
        no-clear;
        no-rescue;
        craft-lockout;
    }
    fpc slot-number {
        port-mirror-instance pm-instance-name;
        power (off | on);
            pic pic-number {
                port-mirror-instance pm-instance-name;
                framing (t1 | e1);
                adaptive-services {
```

```
            service-package (layer-2 | layer-3);
        }
        aggregate-ports;
        atm-cell-relay-accumulation;
        atm-l2circuit-mode (cell | aal5 | trunk trunk);
        vtmapping number;
        ce1 {
            e1 port-number {
                channel-group group-number timeslots slot-number;
            }
        }
        ct3 {
            port port-number {
                t1 link-number {
                    channel-group group-number timeslots slot-number;
                }
            }
        }
        framing (sdh | sonet);
        idle-cell-format {
            itu-t;
            payload-pattern payload-pattern-byte;
        }
        max-queues-per-interface (8 | 4);
        mlfr-uni-nni-bundles number;
        no-concatenate;
        q-pic-large-buffer {
            large-scale;
            small-scale;
        }
        red-buffer-occupancy {
            weighted-averaged [ instant-usage-weight-exponent weight-value ];
        }
    sparse-dlcis;
    traffic-manager {
        ingress-shaping-overhead number;
    mode session-shaping;
    tunnel-services {
    bandwidth (1g | 10g);
    vtmapping (itu-t | klm);
  }
}
fpc-feb-connectivity {
  fpc slot-number feb (slot-number | none);
}
lcc number {
  fpc number {
    pic number {
      atm-cell-relay-accumulation;
      atm-l2circuit-mode (cell | aal5 | trunk trunk);
      framing (sdh | sonet);
      idle-cell-format {
        itu-t;
        payload-pattern payload-pattern-byte;
      }
      max-queues-per-interface (8 | 4);
```

```
            no-concatenate;
          }
        }
        offline;
        online-expected;
    }
    (packet-scheduling | no-packet-scheduling);
    pem {
        minimum number;
    }
    no-concatenate;
    redundancy {
        cfeb slot (always | preferred);
        failover {
            on-disk-failure
            on-loss-of-keepalives;
        }
        feb {
            redundancy-group group-name {
                feb slot-number (backup | primary);
                description description;
                no-auto-failover;
                }
            }
        graceful-switchover;
        keepalive-time seconds;
        routing-engine slot-number (master | backup | disabled);
        sfm slot-number (always | preferred);
        ssb slot-number (always | preferred);
    }
}
network-services (ethernet | ip);
routing-engine {
    on-disk-failure {
        disk-failure-action (halt | reboot);
    }
}
sfm slot-number {
    power off;
}
sib {
    minimum number;
}
vrf-mtu-check;
vtmapping (km | itu-t);
synchronization {
    signal-type (e1 | t1);
    switching-mode (revertive | non-revertive);
    y-cable-line-termination;
    transmitter-enable;
    validation-interval seconds;
    primary (external-a | external-b);
    secondary (external-a | external-b);
}
```

**NOTE:** The configuration statements at the [edit chassis lcc] hierarchy level apply only to a routing matrix. For information about a routing matrix, see "TX Matrix Platform and T640 Routing Node Configuration Guidelines" on page 779 and the *TX Matrix Platform Hardware Guide*.

This chapter describes the following tasks for configuring the router chassis:

## Minimum Chassis Configuration

All of the statements at the [edit chassis] hierarchy level of the configuration are optional.

## Configuring a Flexible PIC Concentrator to Stay Offline

By default, a Flexible PIC Concentrator (FPC) is configured to restart after a system reboot. To configure an FPC to stay offline and prevent it from restarting, include the power off statement at the [edit chassis fpc *slot-number*] hierarchy level:

```
[edit chassis fpc slot-number]
power off;
```

**NOTE:** You can use the request chassis fpc operational mode command to take an FPC offline, but the FPC attempts to restart when you enter a commit CLI command.

To bring an FPC online that is configured to stay offline and configure it to stay online, include the power on statement at the [edit chassis fpc *slot-number*] hierarchy level:

```
[edit chassis fpc slot-number]
power on;
```

## Configuring an SFM to Stay Offline

By default, if you use the request chassis sfm CLI command to take an SFM offline, the SFM attempts to restart when you enter a commit CLI command. To prevent a restart, you can configure an SFM to stay offline. This feature is useful for repair situations.

To configure an SFM to stay offline, include the sfm statement at the [edit chassis] hierarchy level:

```
[edit chassis]
sfm slot-number {
   power off;
}
```

- *slot number*—Slot number in which the SFM is installed.
- power off—Take the SFM offline and configure it to remain offline.

For example, the following statement takes an SFM in slot 3 offline:

```
[edit chassis]
sfm 3 power off;
```

Use the show chassis sfm CLI command to confirm the offline status:

```
user@host# show chassis sfm
                 Temp    CPU Utilization (%) Memory Utilization (%)
Slot    State    (C)     Total   Interrupt   DRAM (MB)   Heap   Buffer
0       Online   34      2       0           64          16     47
1       Online   38      2       0           64          16     47
2       Online   42      2       0           64          16     47
3       Offline --- Configured power off ---
```

To bring the SFM back online, delete the edit chassis sfm statement and then commit the configuration.

## Configuring Aggregated Devices

JUNOS software supports the aggregation of physical devices into defined virtual links, such as the link aggregation of Ethernet interfaces defined by the IEEE 802.3ad standard.

For more information on physical and logical interfaces using aggregated links, including sample configurations, see the *JUNOS Network Interfaces Configuration Guide*.

### *Configuring Virtual Links for Aggregated Devices*

To define the virtual links, you need to specify the associations between physical and logical devices within the [edit interfaces] hierarchy, and assign the correct number of logical devices by including the device-count statement at the [edit chassis aggregated-devices ethernet] and [edit chassis aggregated-devices sonet] hierarchy levels:

```
[edit chassis]
aggregated-devices {
    ethernet {
        device-count number;
    }
    sonet {
        device-count number;
    }
}
```

The maximum number of Ethernet logical interfaces you can configure is 128. The aggregated Ethernet interfaces are numbered from ae0 through ae127. The maximum number of SONET/SDH logical interfaces is 16. The aggregated SONET/SDH interfaces are numbered from as0 through as15.

### *Configuring LACP Link Protection at the Chassis Level*

Link Aggregation Control Protocol (LACP) is one method of bundling several physical interfaces to form one logical interface. You can configure both VLAN-tagged and untagged aggregated Ethernet with or without LACP enabled. LACP exchanges are made between actors and partners. An actor is the local interface in an LACP exchange. A partner is the remote interface in an LACP exchange.

LACP link protection enables you to force active and standby links within an aggregated Ethernet. You configure LACP link protection by configuring the link-protection and system-priority statements at either the chassis or interface level and by configuring port priority at the interface level using the port-priority statement. Configuring LACP parameters at the chassis level results in all aggregated Ethernet interfaces using these values unless overridden by LACP configuration on a specific interface.

```
[edit chassis]
aggregated-devices {
   ethernet {
      lacp {
         link-protection {
            non-revertive;
         }
         system-priority priority;
      }
   }
}
```

You configure LACP link protection by using the link-protection and system-priority statements and define port priority at the port level using the port-priority statement. Configuring LACP parameters at the chassis level results in all aggregated Ethernet interfaces using the defined configuration unless overridden on a specific interface.

**NOTE:** LACP link protection also uses port priority. You can configure port priority at the Ethernet interface [gigether-options] hierarchy level using the port-priority statement. If you choose not to configure port priority, LACP link protection uses the default value for port priority (127). See the *JUNOS Network Interfaces Configuration Guide* for detailed information about LACP and how to configure it on individual aggregated Ethernet interfaces.

**Related Topics** ■ *JUNOS Network Interfaces Configuration Guide*

### *Enabling LACP Link Protection*

To enable LACP link protection for aggregated Ethernet interfaces on the chassis, use the link-protection statement at the [edit chassis aggregated-devices ethernet lacp] hierarchy level:

```
[edit chassis aggregated-devices ethernet lacp]
link-protection {
   non-revertive;
```

}

By default, LACP link protection reverts to a higher-priority (lower-numbered) link when that higher-priority link becomes operational or a link is added to the aggregator that is determined to be higher in priority. However, you can suppress link calculation by adding the non-revertive statement to the LACP link protection configuration. In non-revertive mode, once a link is active and collecting and distributing packets, the subsequent addition of a higher-priority (better) link does not result in a switch, and the current link remains active.

**CAUTION:** If both ends of an aggregator have LACP link protection enabled, make sure to configure both ends of the aggregator to use the same mode. Mismatching LACP link protection modes can result in lost traffic.

### *Configuring System Priority*

To configure LACP system priority for aggregated Ethernet interfaces on the chassis, use the system-priority statement at the [edit chassis aggregated-devices ethernet lacp] hierarchy level:

```
[edit chassis aggregated-devices ethernet lacp]
system-priority priority;
```

The system priority is a 2-octet binary value that is part of the LACP system ID. The LACP system ID consists of the system priority as the two most-significant octets and the interface MAC address as the six least-significant octets. The system with the numerically lower value for system priority has the higher priority. By default, system priority is 127, with a range of 0 to 65535.

## Configuring ATM Cell-Relay Accumulation Mode on an ATM1 PIC

You can configure an Asynchronous Transfer Mode (ATM) 1 PIC to use cell-relay accumulation mode. In this mode, the incoming cells (one to eight cells) are packaged into a single packet and forwarded to the label-switched path (LSP). At the edge router, this packet is divided in to individual cells and transmitted over the ATM interface.

**NOTE:** When you configure an ATM PIC to use cell-relay accumulation, all ports on the ATM PIC use cell-relay accumulation mode.

To configure an ATM PIC to use cell-relay accumulation mode, include the atm-cell-relay-accumulation statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ]
atm-cell-relay-accumulation;
```

On a TX Matrix platform, include the atm-cell-relay-accumulation statement at the [edit chassis lcc *number* fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number]
atm-cell-relay-accumulation;
```

For more information about configuring a TX Matrix platform, see "TX Matrix Platform and T640 Routing Node Configuration Guidelines" on page 779.

## Configuring Port Mirroring Instances on MX-series Routers

You can configure port mirroring for Layer 2 VPLS traffic on MX-series routers. To configure port mirroring, include the vpls statement at the [edit forwarding-options port-mirroring] hierarchy level.

You can configure multiple instances of port mirroring to enable multiple Packet Forwarding Engines to mirror packets to different destinations. To configure multiple instances, include the instance *instance-name* statement at the [edit forwarding-options port-mirroring] hierarchy level.

To configure a router to sample the packet for port mirroring only once, include the mirror-once statement at the [edit forwarding-options]. This option is useful when you are performing port mirroring on both the ingress and egress interfaces to eliminate duplication when input and output filtering is performed on the same packet.

### *Configuring Port Mirroring Instances at the DPC Level on MX-series Routers*

To bind a port-mirroring instance to a specific DPC and its Packet Forwarding Engines, include the port-mirror-instance *pm-instance-name* statement at the [edit chassis fpc *number*] hierarchy level. A port-mirror instance configured at the FPC-level for the DPC is bound to all the Packet Forwarding Engines on the DPC. This overrides the global port mirroring properties (if the port-mirroring statement has been included at the [edit forwarding-options] hierarchy level).

```
[edit chassis]
fpc slot-number {
    port-mirror-instance pm-instance-name;
}
```

### *Configuring Port Mirroring Instances at the PIC Level on MX-series Routers*

For MX-series routers, there is a one-to-one mapping of the Packet Forwarding Engines and the PICs. Therefore, you can override the port mirroring instance properties configured at the DPC level and configure a PIC-level port-mirroring instance. To bind a port mirroring instance to a specific Packet Forwarding Engine and its associated ports, include the include the port-mirror-instance *pm-instance-name* statement at the [edit chassis fpc *slot-number* pic *number*] hierarchy level.

```
[edit chassis]
fpc slot-number {
    port-mirror-instance pm-instance-name-a;
    pic slot-number {
        port-mirror-instance pm-instance-name-b;
    }
}
```

### *Precedence of Port-Mirroring Instances at Different Levels of the Chassis*

If port-mirroring instances are configured at multiple levels in the MX-series router hierarchy, the port-mirroring properties are applied as follows:

1. For chassis-level Layer 2 port mirroring, configured by including the port-mirroring statement at the [edit forwarding-options] hierarchy level, the global port-mirroring properties apply to all DPCs and their Packet Forwarding Engines and their associated ports.
2. For a DPC bound to a named port-mirroring instance, configured by including the port-mirror-instance *pm-instance-name* statement at the [edit chassis fpc *slot-number*] hierarchy level, the FPC-level port mirroring properties apply to all Packet Forwarding Engines (and their associated ports) on the DPC and override the properties of the global port-mirroring instance (if the port-mirroring statement has been included at the [edit forwarding-options] hierarchy level).
3. For a Packet Forwarding Engine bound to a Layer 2 port-mirroring instance (configured by including the port-mirror-instance *pm-instance-name-b* statement at the [edit chassis fpc *slot-number* pic *slot-number*] hierarchy level), the PIC-level port-mirroring properties apply to all ports associated with the Packet Forwarding Engine and override the properties bound to the DPC (if the port-mirror-instance *pm-instance-name-a* statement has been included at the [edit chassis fpc *slot-number*] hierarchy level).

For more information about configuring port mirroring for Layer 2 VPLS traffic, see the *JUNOS MX-series Layer 2 Configuration Guide*.

## Configuring 12-Port T1/E1 Circuit Emulation PICs

The M7i, M10i, and M40e routers support 12-port T1/E1 PICs, primarily used for wireless backhaul applications. The 12-port PIC can be configured for either 12 T1 or 12 E1 interfaces, but not a combination of both interface types.

To configure support for 12-port T1/E1 PICs, include the framing t1 or framing e1 statements respectively at the [edit chassis fpc *slot-number* pic *slot-number* hierarchy level:

```
[edit chassis fpc fpc-slot-number pic pic-slot-number]
framing (t1 | e1);
```

When the PIC comes online, 12 CT1 or CE1 interfaces are created depending on the interface type (T1 or E1) you include in the framing statement.

To configure the T1 or E1 interfaces, include the interface-type t1 statement at the [edit interfaces ct1-*fpc/pic/port* no-partition] hierarchy level or the interface-type ce1 statement at the [edit interfaces ce1-*fpc/pic/port* no-partition] hierarchy level.

To view a list of 12-port T1/E1 PICs, issue the show chassis hardware command. To view the details of a specific PIC, issue the show chassis pic fpc-slot *slot-number* pic-slot *slot-number* command.

For further information about configuring the CT1 and CE1 interfaces, see the *JUNOS Network Interfaces Configuration Guide*

## Configuring Conditions That Trigger Alarms

For the different types of PICs, you can configure which conditions trigger alarms and whether they trigger a red or yellow alarm. Red alarm conditions light the RED ALARM LED on the router's craft interface and trigger an audible alarm if one is connected to the contacts on the craft interface. Yellow alarm conditions light the YELLOW ALARM LED on the router's craft interface and trigger an audible alarm if one is connected to the craft interface.

**NOTE:** By default, any failure condition on the integrated-services interface (Adaptive Services PIC) triggers a red alarm.

To configure conditions that trigger alarms and that can occur on any interface of the specified type, include the alarm statement at the [edit chassis] hierarchy level.

```
[edit chassis]
alarm {
    interface-type {
        alarm-name (red | yellow | ignore);
    }
}
```

*alarm-name* is the name of an alarm.

Table 44 on page 718 lists the systemwide alarms and the alarms for each interface type.

**Table 44: Configurable PIC Alarm Conditions**

| Interface/System | Alarm Condition | Configuration Option |
|---|---|---|
| **SONET/SDH and ATM** | Link alarm indication signal | ais-l |
| | Path alarm indication signal | ais-p |
| | Signal degrade (SD) | ber-sd |
| | Signal fail (SF) | ber-sf |
| | Loss of cell delineation (ATM only) | locd |
| | Loss of framing | lof |
| | Loss of light | lol |
| | Loss of pointer | lop-p |
| | Loss of signal | los |
| | Phase locked loop out of lock | pll |
| | Synchronous transport signal (STS) payload label (C2) mismatch | plm-p |
| | Line remote failure indication | rfi-l |
| | Path remote failure indication | rfi-p |
| | STS path (C2) unequipped | uneq-p |
| **E3/T3** | Alarm indicator signal | ais |
| | Excessive numbers of zeros | exz |
| | Failure of the far end | ferf |
| | Idle alarm | idle |
| | Line code violation | lcv |
| | Loss of frame | lof |
| | Loss of signal | los |
| | Phase locked loop out of lock | pll |
| | Yellow alarm | ylw |
| **Ethernet** | Link has gone down | link-down |
| **DS1** | Alarm indicator signal | ais |
| | Yellow alarm | ylw |

**Table 44: Configurable PIC Alarm Conditions** *(continued)*

| Interface/System | Alarm Condition | Configuration Option |
|---|---|---|
| **Integrated-services** | Hardware or software failure | failure |
| **Management-Ethernet** | Link has gone down | link-down |

## *Chassis Conditions That Trigger Alarms*

Various conditions related to the chassis components trigger yellow and red alarms. You cannot configure these conditions. Table 45 on page 719 through Table 52 on page 743 list the alarms that the chassis components can generate. For information about chassis alarms for J-series Services Routers, see the *J-series Services Router Administration Guide*. For information about chassis alarms for the TX Matrix platform, see the *TX Matrix Platform Hardware Guide*.

Table 45 on page 719 lists the alarms that the chassis components can generate on an M5 or M10 Internet router.

**Table 45: Chassis Components Alarm Conditions on an M5 or M10 Router**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at<br><br>www.juniper.net/<br><br>or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Craft interface** | The craft interface has failed. | Replace failed craft interface. | Red |
| **Fan trays** | One fan tray has been removed from the chassis. | Install missing fan tray. | Yellow |
| | Two or more fan trays have been removed from the chassis. | Install missing fan trays. | Red |
| | One fan in the chassis is not spinning or is spinning below required speed. | Replace failed fan tray. | Red |
| **Forwarding Engine Board (FEB)** | The control board has failed. If this occurs, the board attempts to reboot. | Replace failed FEB. | Red |

**Table 45: Chassis Components Alarm Conditions on an M5 or M10 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Flexible PIC Concentrator (FPC)** | An FPC has failed. If this occurs, the FPC attempts to reboot. If the FEB sees that an FPC is rebooting too often, it shuts down the FPC. | Replace failed FPC. | Red |
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken. | Replace failed component. | Red |
| **Routing Engine** | Error in reading or writing CompactFlash card. | Reformat CompactFlash card and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. | Install bootable image on CompactFlash card. If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| **Power supplies** | A power supply has been removed from the chassis. | Install missing power supply. | Yellow |
| | A power supply has failed. | Replace failed power supply. | Red |

**Table 45: Chassis Components Alarm Conditions on an M5 or M10 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at<br>www.juniper.net/<br>or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

Table 46 on page 722 lists the alarms that the chassis components can generate on an M7i or M10i Internet router.

**Table 46: Chassis Components Alarm Conditions on an M7i or M10i Router**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Compact FEB (CFEB)** | For an M7i router, CFEB has failed. If this occurs, the board attempts to reboot. | Replace failed CFEB. | Red |
| | For an M10i router, both control boards have been removed or have failed. | Replace failed or missing CFEB. | Red |
| | Too many hard errors in CFEB memory. | Replace failed CFEB. | Red |
| | Too many soft errors in CFEB memory. | Replace failed CFEB. | Red |
| | A CFEB microcode download has failed. | Replace failed CFEB. | Red |
| **Fan trays** | A fan has failed. | Replace failed fan tray. | Red |
| | For an M7i router, a fan tray has been removed from the chassis. | Install missing fan tray. | Red |
| | For an M10i router, both fan trays are absent from the chassis. | Install missing fan tray. | Red |
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's midplane from the front is broken. | Replace failed component. | Red |

**Table 46: Chassis Components Alarm Conditions on an M7i or M10i Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Power supplies** | A power supply has been removed. | Insert missing power supply. | Yellow |
| | A power supply has failed. | Replace failed power supply. | Red |
| | For an M10i router, only one power supply is operating. | Insert or replace secondary power supply. | Red |
| **Routing Engine** | Error in reading or writing hard disk. | Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | Error in reading or writing CompactFlash card. | Reformat CompactFlash card and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. This alarm only applies, if you have an optional CompactFlash card. | Install bootable image on CompactFlash card. If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| | Routing Engine failed to boot. | Replace failed Routing Engine. | Red |

**Table 46: Chassis Components Alarm Conditions on an M7i or M10i Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

Table 47 on page 725 lists the alarms that the chassis components can generate on an M20 Internet router.

**Table 47: Chassis Components Alarm Conditions for an M20 Router**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Craft interface** | The craft interface has failed. | Replace failed craft interface. | Red |
| **Fan trays** | One fan tray has been removed from the chassis. | Install missing fan tray. | Yellow |
| | Two or more fan trays have been removed from the chassis. | Install missing fan trays. | Red |
| | One fan in the chassis is not spinning or is spinning below requires speed. | Replace fan tray. | Red |
| **FPC** | An FPC has failed. If this occurs, the FPC attempts to reboot. If the System and Switch Board (SSB) sees that an FPC is rebooting too often, it shuts down the FPC. | Replace failed FPC. | Red |
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs in to the router's backplane from the front (generally, an FPC) is broken. | Replace failed component. | Red |

**Table 47: Chassis Components Alarm Conditions for an M20 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Routing Engine** | Error in reading or writing hard disk. | Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | Error in reading or writing CompactFlash card. | Reformat CompactFlash card and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition. | Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. | Install bootable image on CompactFlash . If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| | Routing Engine failed to boot. | Replace failed Routing Engine. | Red |
| **Power supplies** | A power supply has been removed from the chassis. | Insert power supply into empty slot. | Yellow |
| | A power supply has failed. | Replace failed power supply. | Red |
| **SSB** | The control board has failed. If this occurs, the board attempts to reboot. | Replace failed control board. | Red |

**Table 47: Chassis Components Alarm Conditions for an M20 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

Table 48 on page 728 lists the alarms that the chassis components can generate on an M120 router.

**Table 48: Chassis Component Alarm Conditions for an M120 Router**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Air filters** | Change air filter. | Change air filter. | Yellow |
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Control Board (CB)** | A CB Ethernet switch has failed. | Replace failed CB. | Yellow |
| | A CB has been removed. | Insert CB into empty slot. | Red |
| | A CB has failed. | Replace failed CB. | Red |
| **Craft interface** | The craft interface has failed. | Replace failed craft interface. | Red |
| **Fan trays** | One fan tray has been removed from the chassis. | Install missing fan tray. | Yellow |
| | Two or more fan trays have been removed from the chassis. | Install missing fan trays. | Red |
| | One fan in the chassis is not spinning or is spinning below required speed. | Replace fan tray. | Red |
| **Forwarding Engine Boards (FEBs)** | A spare FEB has failed. | Replace failed FEB. | Yellow |
| | A spare FEB has been removed. | Insert FEB into empty slot. | Yellow |
| | A FEB is offline. | Check FEB. Remove and reinsert the FEB. If this fails, replace failed FEB. | Yellow |
| | A FEB has failed. | Replace failed FEB. | Red |
| | A FEB has been removed. | Insert FEB into empty slot. | Red |
| **Host subsystem** | A host subsystem has failed. | Replace the host subsystem. | Yellow |
| | A host subsystem has been removed. | Insert host subsystem into empty slot. | Red |

**Table 48: Chassis Component Alarm Conditions for an M120 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken. | Replace failed component. | Red |
| **Power supplies** | A power supply has been removed from the chassis. | Insert power supply into empty slot. | Yellow |
| | A power supply has a high temperature. | Replace failed power supply or power entry module. | Red |
| | A power supply input has failed. | Check power supply input connection. | Red |
| | A power supply output has failed. | Check power supply output connection. | Red |
| | A power supply has failed. | Replace failed power supply. | Red |
| **Routing Engine** | Error in reading or writing hard disk. | Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | Error in reading or writing CompactFlash card. | Reformat CompactFlash and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition. | Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. | Install bootable image on CompactFlash card. If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| | Routing Engine failed to boot. | Replace failed Routing Engine. | Red |

**Table 48: Chassis Component Alarm Conditions for an M120 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | Chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

Table 49 on page 731 lists the alarms that the chassis components can generate on an M40 Internet router.

**Table 49: Chassis Component Alarm Conditions for an M40 Router**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Air filter** | Change air filter. | Change air filter. | Yellow |
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Craft interface** | The craft interface has failed. | Replace failed craft interface. | Red |
| **Fan trays** | One fan tray has been removed from the chassis. | Install missing fan tray. | Yellow |
| | Two or more fan trays have been removed from the chassis. | Install missing fan trays. | Red |
| | One fan in the chassis is not spinning or is spinning below required speed. | Replace fan tray. | Red |
| **FPC** | An FPC has an out of range or invalid temperature reading. | Replace failed FPC. | Yellow |
| | An FPC microcode download has failed. | Replace failed FPC. | Red |
| | An FPC has failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC. | Replace failed FPC. | Red |
| | Too many hard errors in FPC memory. | Replace failed FPC. | Red |
| | Too many soft errors in FPC memory. | Replace failed FPC. | Red |
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken. | Replace failed component. | Red |

**Table 49: Chassis Component Alarm Conditions for an M40 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Power supplies** | A power supply has been removed from the chassis. | Insert power supply into empty slot. | Yellow |
| | A power supply temperature sensor has failed. | Replace failed power supply or power entry module. | Yellow |
| | A power supply fan has failed. | Replace failed power supply fan. | Yellow |
| | A power supply has high temperature. | Replace failed power supply or power entry module. | Red |
| | A 5-V power supply has failed. | Replace failed power supply or power entry module. | Red |
| | A 3.3-V power supply has failed. | Replace failed power supply or power entry module. | Red |
| | A 2.5-V power supply has failed. | Replace failed power supply or power entry module. | Red |
| | A power supply input has failed. | Check power supply input connection. | Red |
| | A power supply has failed. | Replace failed power supply or power entry module. | Red |

**Table 49: Chassis Component Alarm Conditions for an M40 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Routing Engine** | Error in reading or writing hard disk. | Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | Error in reading or writing CompactFlash card. | Reformat CompactFlash and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition. | Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. | Install bootable image on CompactFlash card. If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| | Routing Engine failed to boot. | Replace failed Routing Engine. | Red |
| **SCB** | The System Control Board (SCB) has failed. If this occurs, the board attempts to reboot. | Replace failed SCB. | Red |

**Table 49: Chassis Component Alarm Conditions for an M40 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

Table 50 on page 735 lists the alarms that the chassis components can generate on an M40e or M160 Internet router.

**Table 50: Chassis Component Alarm Conditions for an M40e or M160 Router**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Air filter** | Change air filter. | Change air filter | Yellow |
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Connector Interface Panel (CIP)** | A CIP is missing. | Insert CIP into empty slot. | Red |
| **Craft interface** | The craft interface has failed. | Replace failed craft interface. | Red |
| **Fan trays** | One fan tray has been removed from the chassis. | Install missing fan tray. | Yellow |
| | Two or more fan trays have been removed from the chassis. | Install missing fan trays. | Red |
| | One fan in the chassis is not spinning or spinning below required speed. | Replace fan tray. | Red |
| **FPC** | An FPC has an out of range or invalid temperature reading. | Replace failed FPC. | Yellow |
| | An FPC microcode download has failed. | Replace failed FPC. | Red |
| | An FPC has failed. If this occurs, the FPC attempts to reboot. If the MCS sees that an FPC is rebooting too often, it shuts down the FPC. | Replace failed FPC. | Red |
| | Too many hard errors in FPC memory. | Replace failed FPC. | Red |
| | Too many soft errors in FPC memory. | Replace failed FPC. | Red |

**Table 50: Chassis Component Alarm Conditions for an M40e or M160 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken. | Replace failed component. | Red |
| **Miscellaneous Control Subsystem (MCS)** | An MCS has an out of range or invalid temperature reading. | Replace failed MCS. | Yellow |
| | MCS0 has been removed. | Reinstall MCS0. | Yellow |
| | An MCS has failed. | Replace failed MCS. | Red |
| **Packet Forwarding Engine Clock Generator (PCG)** | A backup PCG is offline. | Set backup PCG online. | Yellow |
| | A PCG has an out of range or invalid temperature reading. | Replace failed PCG. | Yellow |
| | A PCG has been removed. | Insert PCG into empty slot. | Yellow |
| | A PCG has failed to come online. | Replace failed PCG. | Red |

**Table 50: Chassis Component Alarm Conditions for an M40e or M160 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Routing Engine** | Error in reading or writing hard disk. | Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | Error in reading or writing CompactFlash card. | Reformat CompactFlash and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition. | Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. | Install bootable image on CompactFlash card. If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| | Routing Engine failed to boot. | Replace failed Routing Engine. | Red |
| **Power supplies** | A power supply has been removed from the chassis. | Insert power supply into empty slot. | Yellow |
| | A power supply has failed. | Replace failed power supply. | Red |
| **Switching and Forwarding Module (SFM)** | An SFM has an out of range or invalid temperature reading on SPP. | Replace failed SFM. | Yellow |
| | An SFM has an out of range or invalid temperature reading on SPR. | Replace failed SFM. | Yellow |
| | An SFM is offline. | Set SFM online. | Yellow |
| | An SFM has failed. | Replace failed SFM. | Red |
| | An SFM has been removed from the chassis. | Insert SFM into empty slot. | Red |
| | All SFMs are offline or missing from the chassis. | Insert SFMs into empty slots or set all SFMs online. | Red |

**Table 50: Chassis Component Alarm Conditions for an M40e or M160 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

Table 51 on page 739 lists the alarms that the chassis components can generate on an M320 Internet router.

**Table 51: Chassis Component Alarm Conditions for an M320 Router**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Air filters** | Change air filter. | Change air filter. | Yellow |
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Control Board (CB)** | A CB has been removed. | Insert CB into empty slot. | Yellow |
| | A CB temperature sensor alarm has failed. | Replace failed CB. | Yellow |
| | A CB has failed. | Replace failed CB. | Red |
| **CIP** | A CIP is missing. | Insert CIP into empty slot. | Red |
| **Craft interface** | The craft interface has failed. | Replace failed craft interface. | Red |
| **Fan trays** | One fan tray has been removed from the chassis. | Install missing fan tray. | Yellow |
| | Two or more fan trays have been removed from the chassis. | Install missing fan trays. | Red |
| | One fan in the chassis is not spinning or is spinning below required speed. | Replace fan tray. | Red |

**Table 51: Chassis Component Alarm Conditions for an M320 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **FPC** | An FPC has an out of range or invalid temperature reading. | Replace failed FPC. | Yellow |
| | An FPC microcode download has failed. | Replace failed FPC. | Red |
| | An FPC has failed. If this occurs, the FPC attempts to reboot. If the CB sees that an FPC is rebooting too often, it shuts down the FPC. | Replace failed FPC. | Red |
| | Too many hard errors in FPC memory. | Replace failed FPC. | Red |
| | Too many soft errors in FPC memory. | Replace failed FPC. | Red |
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken. | Replace failed component. | Red |
| **Power supplies** | A power supply has been removed from the chassis. | Insert power supply into empty slot. | Yellow |
| | A power supply has failed. | Replace failed power supply. | Red |

**Table 51: Chassis Component Alarm Conditions for an M320 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Routing Engine** | Error in reading or writing hard disk. | Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | Error in reading or writing CompactFlash card. | Reformat CompactFlash and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition. | Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. | Install bootable image on CompactFlash card. If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| | Routing Engine failed to boot. | Replace failed Routing Engine. | Red |
| **Switch Interface Board (SIB)** | A spare SIB is missing. | Insert spare SIB in to empty slot. | Yellow |
| | A SIB has failed. | Replace failed SIB. | Yellow |
| | A spare SIB has failed. | Replace failed SIB. | Yellow |
| | A SIB has an out of range or invalid temperature reading. | Replace failed SIB. | Yellow |
| | A SIB is missing. | Insert SIB into empty slot. | Red |
| | A SIB has failed. | Replace failed SIB. | Red |

**Table 51: Chassis Component Alarm Conditions for an M320 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | Chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

Table 52 on page 743 lists the alarms that the chassis components can generate on a T320 or T640 Internet routing platform.

**Table 52: Chassis Component Alarm Conditions for the T320 or T640 Routing Platform**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Air filter** | Change air filter. | Change air filter. | Yellow |
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **CB** | A CB has been removed. | Insert CB into empty slot. | Yellow |
| | A CB temperature sensor alarm has failed. | Replace failed CB. | Yellow |
| | A CB has failed. | Replace failed CB. | Red |
| **CIP** | A CIP is missing. | Insert CIP into empty slot. | Red |
| **Craft interface** | The craft interface has failed. | Replace failed craft interface. | Red |
| **Fan trays** | One fan tray has been removed from the chassis. | Install missing fan tray. | Yellow |
| | Two or more fan trays have been removed from the chassis. | Install missing fan trays. | Red |
| | One fan in the chassis is not spinning or is spinning below required speed. | Replace fan tray. | Red |
| **FPC** | An FPC has an out of range or invalid temperature reading. | Replace failed FPC. | Yellow |
| | An FPC microcode download has failed. | Replace failed FPC. | Red |
| | An FPC has failed. If this occurs, the FPC attempts to reboot. If the CB sees that an FPC is rebooting too often, it shuts down the FPC. | Replace failed FPC. | Red |
| | Too many hard errors in FPC memory. | Replace failed FPC. | Red |
| | Too many soft errors in FPC memory. | Replace failed FPC. | Red |

**Table 52: Chassis Component Alarm Conditions for the T320 or T640 Routing Platform** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken. | Replace failed component. | Red |
| **Routing Engine** | Error in reading or writing hard disk. | Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | Error in reading or writing CompactFlash card. | Reformat CompactFlash and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition. | Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. | Install bootable image on CompactFlash. If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| | Routing Engine failed to boot. | Replace failed Routing Engine. | Red |
| **Power supplies** | A power supply has been removed from the chassis. | Insert power supply into empty slot. | Yellow |
| | A power supply has failed. | Replace failed power supply. | Red |

**Table 52: Chassis Component Alarm Conditions for the T320 or T640 Routing Platform** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **SONET Clock Generator (SCG)** | A backup SCG is offline. | Set backup SCG online. | Yellow |
| | An SCG has an out of range or invalid temperature reading. | Replace failed SCG. | Yellow |
| | An SCG has been removed. | Insert SCG into empty slot. | Yellow |
| | All SCGs are offline or missing. | Insert SCGs into empty slots or set all SCGs online. | Red |
| | An SCG has failed. | Replace failed SCG. | Red |
| **SIB** | A spare SIB is missing. | Insert spare SIB into empty slot. | Yellow |
| | A SIB has failed. | Replace failed SIB. | Yellow |
| | A spare SIB has failed. | Replace failed SIB. | Yellow |
| | A SIB has an out of range or invalid temperature reading. | Replace failed SIB. | Yellow |
| | A SIB is missing. | Insert SIB into empty slot. | Red |
| | A SIB has failed. | Replace failed SIB. | Red |
| **Switch Processor Mezzanine Board (SPMB)** | A local SPMB is offline. | Reset control board. If this fails, replace control board. | Red |

**Table 52: Chassis Component Alarm Conditions for the T320 or T640 Routing Platform** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | Chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

Table 53 on page 747 lists the alarms that the chassis components can generate on an MX-series router.

**Table 53: Chassis Component Alarm Conditions for an MX240, MX480, or MX960 Router**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Air filters** | Change air filter. | Change air filter. | Yellow |
| **Alternative media** | The router boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Craft interface** | The craft interface has failed. | Replace failed craft interface. | Red |
| **Dense Port Concentrators (DPC)s** | A DPC is offline. | Check DPC. Remove and reinsert the DPC. If this fails, replace failed DPC. | Yellow |
| | A DPC has failed. | Replace failed DPC. | Red |
| | A DPC has been removed. | Insert DPC into empty slot. | Red |
| **Fan trays** | A fan tray has been removed from the chassis. | Install missing fan tray. | Red |
| | One fan in the chassis is not spinning or is spinning below required speed. | Replace fan tray. | Red |
| **Host subsystem** | A host subsystem has been removed. | Insert host subsystem into empty slot. | Yellow |
| | A host subsystem has failed. | Replace failed host subsystem. | Red |
| **Hot swapping** | Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken. | Replace failed component. | Red |

**Table 53: Chassis Component Alarm Conditions for an MX240, MX480, or MX960 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Power supplies** | A power supply has been removed from the chassis. | Insert power supply into empty slot. | Yellow |
| | A power supply has a high temperature. | Replace failed power supply or power entry module. | Red |
| | A power supply input has failed. | Check power supply input connection. | Red |
| | A power supply output has failed. | Check power supply output connection. | Red |
| | A power supply has failed. | Replace failed power supply. | Red |
| | Invalid AC power supply configuration. | When two AC power supplies are installed, insert one power supply into an odd-numbered slot and the other power supply into an even-numbered slot. | Red |
| | Invalid DC power supply configuration. | When two DC power supplies are installed, insert one power supply into an odd-numbered slot and the other power supply into an even-numbered slot. | Red |
| | Mix of AC and DC power supplies. | Do not mix AC and DC power supplies. For DC power, remove the AC power supply. For AC power, remove the DC power supply. | Red |
| | Not enough power supplies. | Install an additional power supply. | Red |

**Table 53: Chassis Component Alarm Conditions for an MX240, MX480, or MX960 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Routing Engine** | Error in reading or writing hard disk. | Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | Error in reading or writing CompactFlash card. | Reformat CompactFlash and install bootable image. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition. | Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine. | Yellow |
| | System booted from hard disk. | Install bootable image on CompactFlash card. If this fails, replace failed Routing Engine. | Yellow |
| | CompactFlash card missing in boot list. | Replace failed Routing Engine. | Red |
| | Hard disk missing in boot list. | Replace failed Routing Engine. | Red |
| | Routing Engine failed to boot. | Replace failed Routing Engine. | Red |
| **System Control Board (SCB)** | An SCB has been removed. | Insert SCB into empty slot. | Yellow |
| | An SCB temperature sensor alarm has failed. | Replace failed SCB. | Yellow |
| | An SCB has failed. | Replace failed SCB. | Red |

**Table 53: Chassis Component Alarm Conditions for an MX240, MX480, or MX960 Router** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Temperature** | The chassis temperature has exceeded 55 degrees C (131 degrees F), the fans have been turned on to full speed, and one or more fans have failed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Yellow |
| | The chassis temperature has exceeded 65 degrees C (149 degrees F), and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | Chassis temperature has exceeded 75 degrees C (167 degrees F). If this condition persists for more than 4 minutes, the router shuts down. | ■ Check room temperature.<br>■ Check air filter and replace it.<br>■ Check airflow.<br>■ Check fan. | Red |
| | The temperature sensor has failed. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Red |

### Backup Routing Engine Alarms

For routers with master and backup Routing Engines, a master Routing Engine can generate alarms for events that occur on a backup Routing Engine. Table 54 on page 751 lists chassis alarms generated for a backup Routing Engine.

**NOTE:** Because the failure occurs on the backup Routing Engine, alarm severity for some events (such as Ethernet interface failures) is yellow instead of red.

**NOTE:** For information about configuring redundant Routing Engines, see the *JUNOS High Availability Configuration Guide*.

**Table 54: Backup Routing Engine Alarms**

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Alternative media** | The backup Routing Engine boots from an alternate boot device, the hard disk. The CompactFlash card is typically the primary boot device. The Routing Engine boots from the hard disk when the primary boot device fails. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |
| **Boot Device** | The boot device (CompactFlash or hard disk) is missing in boot list on the backup Routing Engine. | Replace failed backup Routing Engine. | Red |
| **Ethernet** | The Ethernet management interface (fxp0) on the backup Routing Engine is down. | ■ Check the interface cable connection.<br>■ Reboot the system.<br>■ If the alarm recurs, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States) | Yellow |
| **FRU Offline** | The backup Routing Engine has stopped communicating with the master Routing Engine. | Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States). | Yellow |

**Table 54: Backup Routing Engine Alarms** *(continued)*

| Chassis Component | Alarm Condition | Remedy | Alarm Severity |
|---|---|---|---|
| **Hard Disk** | Error in reading or writing hard disk on the backup Routing Engine. | Reformat hard disk and install bootable image. If this fails, replace failed backup Routing Engine. | Yellow |
| **Multibit Memory ECC** | The backup Routing Engine reports a multibit ECC error. | ■ Reboot the system with the board reset button on the backup Routing Engine.<br>■ If the alarm recurs, open a support case using the Case Manager link at www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States) | Yellow |

## *Silencing External Devices*

You can manually silence external devices connected to the alarm relay contacts by pressing the alarm cutoff button located on the craft interface front panel. Silencing the device does not remove the alarm messages from the display (if present on the router) or extinguish the alarm LEDs. In addition, new alarms that occur after an external device is silenced reactivate the external device.

## *Disabling Physical Operation of the Craft Interface*

You can disable the physical operation of the craft interface front panel on the routing platform. When you disable the the operation of the craft interface, the buttons on the front panel, such as the alarm cutoff button, no longer function. To disable the craft interface operation, include the craft-lockout statement at the [edit chassis] hierarchy level:

```
[edit chassis]
craft-lockout;
```

For more information about how to configure the craft interface, see “Configuring Conditions That Trigger Alarms” on page 717.

## Configuring Service Packages on Adaptive Services Interfaces

For Adaptive Services (AS) PICs, MultiServices PICs, and the internal Adaptive Services Module (ASM) in the M7i platform, there are two service packages: Layer 2 and Layer 3. Both service packages are supported on all adaptive services interfaces, but you can enable only one service package per PIC, with the exception of the combined package supported on the ASM. On a single routing platform, you can enable both service packages by installing two or more PICs on the platform.

You enable service packages per PIC, not per port. For example, if you configure the Layer 2 service package, the entire PIC uses the configured package. To enable a service package, include the service-package statement at the [edit chassis fpc *slot-number* pic *pic-number* adaptive-services] hierarchy level, and specify layer-2 or layer-3:

```
[edit chassis fpc slot-number pic pic-number adaptive-services]
service-package (layer-2 | layer-3);
```

To determine which package an AS PIC supports, issue the show chassis hardware command: if the PIC supports the Layer 2 package, it is listed as Link Services II, and if it supports the Layer 3 package, it is listed as Adaptive Services II. To determine which package a MultiServices PIC supports, issue the show chassis pic fpc-slot *slot-number* pic-slot *slot-number* command. The Package field displays the value Layer-2 or Layer-3.

**NOTE:** The ASM has a default option that combines the features available in the Layer 2 and Layer 3 service packages.

After you commit a change in the service package, the PIC is taken offline and then brought back online immediately. You do not need to manually take the PIC offline and online.

**NOTE:** Changing the service package causes all state information associated with the previous service package to be lost. You should change the service package only when there is no active traffic going to the PIC.

The services supported in each package differ by PIC and platform type. For more information, see the "Adaptive Services Overview" chapter in the *JUNOS Services Interfaces Configuration Guide*.

For additional information about Layer 3 services, see the *JUNOS Feature Guide*.

## Configuring Next-Generation SONET Phase I PICs

In JUNOS Release 8.4 and later, the family of next-generation SONET Phase I PICs includes Type 2 and Type 1 PICs. Each PIC type has three varieties.

Type1 PICs include:

- 4-port OC3
- 2-port OC3
- 1-port OC12

Type 2 PICs include:

- 1-port OC48
- 4-port OC12
- 4-port OC3

The support both type 1 and type 2 FPC interfaces. Hot-pluggable SFPs are used as optical transponders. The PICs provide unprecedented flexibility by allowing the user to configure a variety of modes on them through the configuration of concatenation/nonconcatenation and speed.

The 4-port OC48 PIC with SFP installed, the next-generation SONET/SDH PICs with SFP, and the 4-port OC192 PIC on M-series and T-series routing platforms, support SONET or SDH framing on a per-port basis. This functionality allows you to mix SONET and SDH modes on interfaces on a single PIC.

For information about configuring SONET/SDH framing, see "Configuring SONET/SDH Framing" on page 754.

For information about configuring port speed for concatenate mode on a next-generation PIC, see the *JUNOS Hardware Network Operations Guide*.

## Configuring SONET/SDH Framing

By default, SONET/SDH PICs use SONET framing. For a discussion of the differences between the two standards, see the *JUNOS Network Interfaces Configuration Guide*.

To configure a PIC to use SDH framing, include the framing statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level, specifying the sdh option:

```
[edit chassis]
user@host# set fpc  slot-number pic  pic-number framing sdh
[edit chassis]
user@host# show
fpc slot-number {
    pic pic-number {
        framing sdh;
    }
}
```

On a TX Matrix platform, include the framing statement at the [edit chassis lcc *number* fpc *slot-number* pic *pic-number*] hierarchy level, specifying the sdh option:

```
[edit chassis lcc number]
user@host# set fpc slot-number pic pic-number framing sdh
```

```
[edit chassis lcc number]
user@host# show
fpc slot-number {
    pic pic-number {
        framing sdh;
    }
}
```

To explicitly configure a PIC to use SONET framing, include the framing statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level, specifying the sonet option:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number framing sonet
[edit chassis]
user@host# show
fpc slot-number {
    pic pic-number {
        framing sonet;
    }
}
```

On a TX Matrix platform, include the framing statement at the [edit chassis lcc *number* fpc *slot-number* pic *pic-number*] hierarchy level, specifying the sonet option:

```
user@host# set fpc slot-number pic pic-number framing sonet
[edit chassis lcc number]
user@host# show
fpc slot-number {
    pic pic-number {
        framing sonet;
    }
}
```

For information about configuring a TX Matrix platform, see "TX Matrix Platform and T640 Routing Node Configuration Guidelines" on page 779.

## Configuring an External Synchronization Interface

The M320, M40e, and M120 routing platforms support an external synchronization interface that can be configured to synchronize the internal Stratum 3 clock to an external source.

This feature can be configured for external primary and secondary interfaces that use Building Integrated Timing System (BITS), SDH Equipment Timing Source (SETS) timing sources, or an equivalent quality timing source. When internal timing is set for SONET/SDH, Plesiochronous Digital Hierarchy (PDH), or digital hierarchy (DS-1) interfaces on the Physical Interface Cards (PICs), the transmit clock of the interface is synchronized to BITS/SETS timing and is traceable to timing within the network.

To configure external synchronization on the M320, M40e, or M120 router, include the synchronization statement at the [edit chassis] hierarchy level:

```
[edit chassis]
```

```
synchronization {
    signal-type (t1 | e1);
    switching-mode (revertive | non-revertive);
    y-cable-line-termination;
    transmitter-enable;
    validation-interval seconds;
    primary (external-a | external-b);
    secondary (external-a | external-b);
}
```

Use the synchronization statement options to specify a primary and secondary timing source. To do this, configure the following options:

- For the M320 router, specify a signal-type mode for interfaces, either t1 or e1. For the M40e router, only the t1 signal-type mode is supported. The default setting is t1.
- Specify the switching mode as revertive if a lower-priority synchronization can be switched to a valid, higher-priority synchronization.
- For the M320 router, specify that a single signal should be wired to both Control Boards (CBs) using a Y-cable. For the M40e router, the signal is wired to the CIP and Y-cable functionality is embedded in this system.

  The y-cable-line-termination option is not available on the M40e and M120 routers.
- Control whether the diagnostic timing signal is transmitted.

  The transmitter-enable option is not available on the M120 routers.
- Set a validation interval. The validation-interval option validates the synchronized deviation of the synchronization source. If revertive switching is enabled and a higher-priority clock is validated, the clock module is directed to the higher-priority clock, and all configured and active synchronizations are validated. The validation timer resumes after the current validation interval expires. The validation interval can be a value from 90 through 86400 seconds. The default value is 90 seconds. For the M120 router, the range for the validation-interval option is 30 through 86400 and the default value is 30.
- Specify the primary external timing source.
- Specify the secondary external timing source.

## Configuring Sparse DLCI Mode

By default, original channelized DS3 and original channelized STM1-to-E1 (or T1) interfaces can support a maximum of 64 data-link connection identifiers (DLCIs) per channel—as many as 1792 DLCIs per DS3 interface or 4032 DLCIs per STM1 interface (0 through 63).

In sparse DLCI mode, the full DLCI range (1 through 1022) is supported. This allows you to use circuit cross-connect (CCC) and translation cross-connect (TCC) features by means of Frame Relay on T1 and E1 interfaces. For more information about CCC and DLCIs, see the *JUNOS Network Interfaces Configuration Guide*.

**NOTE:** Sparse DLCI mode requires a Channelized STM1 or Channelized DS3 PIC.

DLCI 0 is reserved for Local Management Interface (LMI) signaling.

Channelized T3 (CT3) intelligent queuing (IQ) and STM1 IQ interfaces support a maximum of 64 DLCIs, numbered 0 through 1022, and therefore do not require sparse mode.

The CT3 PIC must use field-programmable gate array (FPGA) hardware revision 17 to run sparse DLCI mode.

To configure the router to use sparse DLCI mode, include the sparse-dlcis statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ]
sparse-dlcis;
```

## Configuring Channelized PIC Operation

By default, SONET PICs (interfaces with names so-*fpc/pic/port*) operate in concatenated mode, a mode in which the bandwidth of the interface is in a single channel.

To configure a PIC to operate in channelized (multiplexed) mode, include the no-concatenate statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number no-concatenate
[edit chassis]
user@host# show
fpc slot-number {
    pic pic-number {
        no-concatenate;
    }
}
```

On a TX Matrix platform, include the no-concatenate statement at the [edit chassis lcc *number* fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis lcc number]
user@host# set fpc slot-number pic pic-number no-concatenate
[edit chassis lcc number]
user@host# show
fpc slot-number {
    pic pic-number {
        no-concatenate;
    }
}
```

When configuring and displaying information about interfaces that are operating in channelized mode, you must specify the channel number in the interface name (*physical:channel*); for example, so-2/2/0:0 and so-2/2/0:1. For more information about interface names, see the *JUNOS Network Interfaces Configuration Guide*. For information about the TX Matrix platform, see "TX Matrix Platform and T640 Routing Node Configuration Guidelines" on page 779.

### *Concatenated and Nonconcatenated Mode*

On SONET OC48 interfaces that are configured for channelized (multiplexed) mode, the bytes e1-quiet and bytes f1 options in the sonet-options statement have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0. These bytes work in the transmit direction only on channels 1, 2, and 3.

The M160 four-port SONET/SDH OC12 PIC can run each of the OC12 links in concatenated mode only and requires a Type 2 M160 FPC. Similarly, the four-port SONET/SDH OC3 PIC cannot run in nonconcatenated mode on any platform.

## Configuring Channelized DS3-to-DS0 Naming

You can configure 28 T1 channels per T3 interface. Each T1 link can have up to eight channel groups, and each channel group can hold any combination of DS0 time slots. To specify the T1 link and DS0 channel group number in the name, use colons (:) as separators. For example, a Channelized DS3-to-DS0 PIC might have the following physical and virtual interfaces:

ds-0/0/0:*x*:*y*

where *x* is a T1 link ranging from 0 through 27 and *y* is a DS0 channel group ranging from 0 through 7. (See Table 55 on page 759 for more information about ranges.)

You can use any of the values within the range available for *x* and *y*; you do not have to configure the links sequentially. The software applies the interface options you configure according to the following rules:

- You can configure t3-options for t1 link 0 and channel group 0 only; for example, ds-/0/0/0:0:0.
- You can configure t1-options for any t1 link value, but only for channel group 0; for example, ds-0/0/0:x:0.
- There are no restrictions on changing the default ds0-options.
- If you delete a configuration you previously committed for channel group 0, the options return to the default values.

To configure the channel groups and time slots for a channelized DS3 interface, include the channel-group and timeslots statements at the [edit chassis fpc slot-number pic *pic-number* ct3 port *port-number* t1 *link-number*] hierarchy level:

[edit chassis fpc *slot-number* pic *pic-number* ct3 port *port-number* t1 *link-number*]
channel-group *group-number* timeslots *slot-number*;

**NOTE:** If you commit the interface name but do not include the [edit chassis] configuration, the Channelized DS3-to-DS0 PIC behaves like a Channelized DS3-to-DS1 PIC: none of the DS0 functionality is accessible.

Table 55 on page 759 shows the ranges for each of the quantities in the preceding configuration.

**Table 55: Ranges for Channelized DS3-to-DS0 Configuration**

| Item | Variable | Range |
|---|---|---|
| FPC slot | *slot-number* | 0 through 7 (see note below) |
| PIC slot | *pic-number* | 0 through 3 |
| Port | *port-number* | 0 through 1 |
| T1 link | *link-number* | 0 through 27 |
| DS0 channel group | *group-number* | 0 through 7 |
| time slot | *slot-number* | 1 through 24 |

**NOTE:** The FPC slot range depends on the platform. The maximum range of 0 through 7 applies to M40 routers; for M20 routers, the range is 0 through 3; for M10 routers the range is 0 through 1; for M5 routers, the only applicable value is 0. The Multichannel DS3 (Channelized DS3-to-DS0) PIC is not supported on M160 routers.

Bandwidth limitations restrict the interface to a maximum of 128 channel groups per T3 port, rather than the theoretical maximum of 8 x 28 = 224.

There are 24 time slots on a T1 interface. You can designate any combination of time slots for usage, but you can use each time slot number on only one channel group within the same T1 link.

To use time slots 1 through 10, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots 1-10;
```

To use time slots 1 through 5, time slot 10, and time slot 24, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots 1-5,10,24;
```

Note that spaces are not allowed when you specify time slot numbers. For more information about these interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

## Configuring Eight Queues on IQ Interfaces

By default, IQ PICs on T-series and M320 routing platforms are restricted to a maximum of four egress queues per interface. To configure a maximum of eight egress queues on IQ interfaces, include the max-queues-per-interface statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
max-queues-per-interface (8 | 4);
```

On a TX Matrix platform, include the max-queues-per-interface statement at the [edit chassis lcc *number* fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number]
max-queues-per-interface (8 | 4);
```

**NOTE:** The configuration at the [edit class-of-service] hierarchy level must also support eight queues per interface.

The maximum number of queues per IQ PIC can be 4 or 8. If you include the max-queues-per-interface statement, all ports on the IQ PIC use configured mode and all interfaces on the IQ PIC have the same maximum number of queues.

If you include the max-queues-per-interface 4 statement, you can configure all four ports and configure up to four queues per port.

For 4-port OC3c/STM1 Type I and Type II PICs on M320 and T-series platforms, when you include the max-queues-per-interface 8 statement, you can configure up to eight queues on ports 0 and 2. After you commit the configuration, the PIC goes offline and comes back online with only ports 0 and 2 operational. No interfaces can be configured on ports 1 and 3.

For Quad T3 and Quad E3 PICs, when you include the max-queues-per-interface 8 statement, you can configure up to eight queues on ports 0 and 2. After you commit the configuration, the PIC goes offline and comes back online with only ports 0 and 2 operational. No interfaces can be configured on ports 1 and 3.

When you include the max-queues-per-interface statement and commit the configuration, all physical interfaces on the IQ PIC are deleted and readded. Also, the PIC is taken offline and then brought back online immediately. You do not need to take the PIC offline and online manually. You should change modes between four queues and eight queues only when there is no active traffic going to the IQ PIC.

For more information about how to configure eight queues on each interface, see the *JUNOS Network Interfaces Configuration Guide*. For information about the TX Matrix platform, see “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 779.

## Configuring Channelized E1 Naming

Each Channelized E1 PIC has 10 E1 ports that you can channelize to the *N*xDS0 level. Each E1 interface has 32 time slots (DS0), in which time slot 0 is reserved. You can combine one or more of these timeslots (DS-0) to create a channel group (*N*xDS-0). There can be a maximum of 32 channel groups per E1 interface. Thus, you can configure as many as 320 channel groups per PIC (10 ports x 32 channel groups per port).

To specify the DS0 channel group number in the interface name, include a colon (:) as a separator. For example, a Channelized E1 PIC might have the following physical and virtual interfaces:

ds-0/0/0:*x*

where *x* is a DS0 channel group ranging from 0 through 23. (See Table 56 on page 761 for more information about ranges.)

You can use any of the values within the range available for *x*; you do not have to configure the links sequentially. The software applies the interface options you configure according to the following rules:

- You can configure the e1-options statement for channel group 0 only; for example, ds-0/0/0:0.
- There are no restrictions on changing the default ds0-options.
- If you delete a configuration you previously committed for channel group 0, the options return to the default values.

To configure the channel groups and time slots for a Channelized E1 interface, include the channel-group and timeslots statements at the [edit chassis fpc *slot-number* pic *pic-number* ce1 e1 *port-number*] hierarchy level:

[edit chassis fpc *slot-number* pic *pic-number* ce1 e1 *port-number*]
channel-group *group-number* timeslots *slot-number*;

**NOTE:** If you commit the interface name but do not include the [edit chassis] configuration, the Channelized E1 PIC behaves like a standard E1 PIC: none of the DS0 functionality is accessible.

Table 56 on page 761 shows the ranges for each of the quantities in the preceding configuration.

**Table 56: Ranges for Channelized E1 Configuration**

| Item | Variable | Range |
|---|---|---|
| FPC slot | *slot-number* | 0 through 7 (see note below) |
| PIC slot | *pic-number* | 0 through 3 |

**Table 56: Ranges for Channelized E1 Configuration** *(continued)*

| Item | Variable | Range |
|---|---|---|
| E1 port | *port-number* | 0 through 9 |
| DS0 channel group | *group-number* | 0 through 23 |
| time slot | *slot-number* | 1 through 32 |

**NOTE:** The FPC slot range depends on the platform. The maximum range of 0 through 7 applies to M40 routers; for M20 routers, the range is 0 through 3; for M10 routers the range is 0 through 1; for M5 routers, the only applicable value is 0. The Channelized E1 PIC is not supported on M160 routers.

The theoretical maximum number of channel groups possible per PIC is 10 x 24 = 240. This is within the maximum bandwidth available.

There are 32 time slots on an E1 interface. You can designate any combination of time slots for usage.

To use time slots 1 through 10, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]
channel-group group-number timeslots 1-10;
```

To use time slots 1 through 5, time slot 10, and time slot 24, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]
channel-group group-number timeslots 1-5,10,24;
```

Note that spaces are not allowed when you specify time slot numbers.

For further information about these interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

## Configuring Channelized STM1 Interface Virtual Tributary Mapping

By default, virtual tributary mapping uses KLM mode. You can configure virtual tributary mapping to use KLM or ITU-T mode. On the original Channelized STM1 PIC, to configure virtual tributary mapping, include the vtmapping statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
vtmapping (klm | itu-t);
```

For the Channelized STM1 PIC with IQ, you can configure virtual tributary mapping by including the vtmapping statement at the [edit interfaces cau4 fpc *slot-number* pic *pic-number* sonet-options] hierarchy level. For more information, see the *JUNOS Network Interfaces Configuration Guide*.

## Configuring ATM2 Intelligent Queuing Layer 2 Circuit Transport Mode

On ATM2 IQ PICs only, you can configure Layer 2 circuit cell relay, Layer 2 circuit ATM Adaptation Layer 5 (AAL5), or Layer 2 circuit trunk mode.

Layer 2 circuit cell relay and Layer 2 circuit AAL5 are defined in the Internet draft draft-martini-l2circuit-encap-mpls-04.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*.

Layer 2 circuit trunk mode allows you to send ATM cells over Multiprotocol Label Switching (MPLS) trunking.

The four transport modes are defined as follows:

- To tunnel IP packets over an ATM backbone, use the default standard AAL5 transport mode.
- To tunnel a stream of AAL5-encoded ATM segmentation-and-reassembly protocol data units (SAR-PDUs) over an MPLS or IP backbone, use Layer 2 circuit AAL5 transport mode.
- To tunnel a stream of ATM cells over an MPLS or IP backbone, use Layer 2 circuit cell-relay transport mode.
- To transport ATM cells over an MPLS core network that is implemented on some other vendor switches, use Layer 2 circuit trunk mode.

**NOTE:** You can transport AAL5-encoded traffic with Layer 2 circuit cell-relay transport mode, because Layer 2 circuit cell-relay transport mode ignores the encoding of the cell data presented to the ingress interface.

When you configure AAL5 mode Layer 2 circuits, the control word carries cell loss priority (CLP) information by default.

By default, ATM2 IQ PICs are in standard AAL5 transport mode. Standard AAL5 allows multiple applications to tunnel the protocol data units of their Layer 2 protocols over an ATM virtual circuit. To configure the Layer 2 circuit transport modes, include the atm-l2circuit-mode statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
atm-l2circuit-mode (cell | aal5 | trunk trunk);
```

On a TX Matrix platform, include the atm-l2circuit-mode statement at the [edit chassis lcc *number* fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number]
```

```
atm-l2circuit-mode (cell | aal5 | trunk trunk);
```

aal5 tunnels a stream of AAL5-encoded ATM cells over an IP backbone.

cell tunnels a stream of ATM cells over an IP backbone.

trunk transports ATM cells over an MPLS core network that is implemented on some other vendor switches. Trunk mode can be user-to-network interface (UNI) or network-to-network interface (NNI).

**NOTE:** To determine which vendors support Layer 2 circuit trunk mode, contact Juniper Networks customer support.

For more information about ATM Layer 2 circuit transport mode, see the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Feature Guide*. For information about the TX Matrix platform, see "TX Matrix Platform and T640 Routing Node Configuration Guidelines" on page 779.

## Enabling ILMI for Cell Relay

Integrated Local Management Interface (ILMI) is supported on AAL5 interfaces, regardless of transport mode. To enable ILMI on interfaces with cell-relay encapsulation, you must configure an ATM2 IQ PIC to use Layer 2 circuit trunk transport mode.

To configure ILMI on an interface with cell-relay encapsulation, include the following statements:

```
[edit chassis fpc slot-number pic pic-number]
atm-l2circuit-mode trunk trunk;
[edit interfaces at-fpc/pic/port]
encapsulation atm-ccc-cell-relay;
atm-options {
    ilmi;
    pic-type atm2;
}
unit logical-unit-number {
    trunk-id number;
}
```

For an example on how to enable ILMI for cell relay, see the *JUNOS Network Interfaces Configuration Guide*.

## Configuring Tunnel Interfaces on MX-Series Ethernet Services Routers

The MX-series routing platforms do not use FPCs. The DPC combines the functions of four FPCs and the PICs. The MX960 has 12 DPC slots. The MX480 has 7 DPC slots. The MX240 has 4 DPC slots. Each DPC has either 40 Gigabit Ethernet ports or 4 10-Gigabit Ethernet ports.

Because the MX-series routers do not support Tunnel PICs, you configure a DPC and corresponding Packet Forwarding Engine to use for tunneling services at the [edit chassis] hierarchy level. You also configure the amount of bandwidth reserved for tunnel services. The JUNOS software creates tunnel interfaces on the Packet Forwarding Engine. To create tunnel interfaces on MX-series routers, include the following statements at the [edit chassis] hierarchy level:

```
[edit chassis]
fpc slot-number {
   pic number {
      tunnel-services {
         bandwidth (1g | 10g);
      }
   }
}
```

fpc *slot-number* is the slot number of the DPC. If two SCBs are installed, the range is 0 through 11. If three SCBs are installed, the range is 0 through 5 and 7 through 11.

pic *number* is the number of the Packet Forwarding Engine on the DPC. The range is 0 through 3.

bandwidth (1g | 10g) is the amount of bandwidth to reserve for tunnel traffic on each Packet Forwarding Engine.

1g indicates that 1 Gbps of bandwidth is reserved for tunnel traffic. Configure this option only for a Packet Forwarding Engine on a Gigabit Ethernet 40-port DPC.

10g indicates that 10 Gbps of bandwidth is reserved for tunnel traffic. Configure this option only for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.

If you specify a bandwidth that is not compatible with the type of DPC and Packet Forwarding Engine, tunnel services are not activated. For example, you cannot specify a bandwidth of 1 Gbps for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.

When you configure tunnel interfaces on the Packet Forwarding Engine of a 10-Gigabit Ethernet 4-port DPC, the Ethernet interfaces for that port are removed from service and are no longer visible in the CLI. The Packet Forwarding Engine of a 10-Gigabit Ethernet 4-port DPC supports either tunnel interfaces or Ethernet interfaces, but not both. Each port on the 10-Gigabit Ethernet 4-port DPC includes two LEDs, one for tunnel services and one for Ethernet services, to indicate which type of service is being used. On the Gigabit Ethernet 40-port DPC, you can configure both tunnel and Ethernet interfaces at the same time.

To verify that the tunnel interfaces have been created, issue the show interfaces terse operational mode command. For more information, see the *JUNOS Interfaces Command Reference*.

For additional information about tunnel services, see the " Tunnel Services" chapter in the *JUNOS Services Interfaces Configuration Guide*.

### *Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC*

In this example, you create tunnel interfaces on Packet Forwarding Engine 1 of DPC 4 with 1 Gbps of bandwidth reserved for tunnel services. On a Gigabit Ethernet 40-port DPC, tunnel interfaces coexist with Ethernet interfaces. With this configuration, the Gigabit Ethernet interfaces are ge-4/1/0 through ge-4/1/9. The tunnel interfaces created are gr-4/1/10, pe-4/1/10, pd-4/1/10, vt-4/1/10 and so on.

```
[edit chassis]
fpc 4 pic 1 {
   tunnel-services {
      1g;
   }
}
```

### *Example: Configuring Tunnel Interfaces on a 10-Gigabit Ethernet 4-Port DPC*

In this example, you create tunnel interfaces on Packet Forwarding Engine 0 of

DPC 4 with 10 Gbps of bandwidth reserved for tunnel traffic. Ethernet and tunnel interfaces cannot coexist on the same Packet Forwarding Engine of a 10-Gigabit Ethernet 4-port DPC. With this configuration, the tunnel interfaces created are gr-4/0/0, pe-4/0/0, pd-4/0/0, vt-4/0/0 and so on.

```
[edit chassis]
fpc 4 pic 0 {
   tunnel-services {
      10g;
   }
}
```

## Configuring Packet Scheduling

By default, packet scheduling is disabled. To configure a router to operate in packet-scheduling mode, include the packet-scheduling statement at the [edit chassis] hierarchy level:

```
[edit chassis]
packet-scheduling;
```

To explicitly disable the packet-scheduling statement, include the no-packet-scheduling statement at the [edit chassis] hierarchy level:

```
[edit chassis]
no-packet-scheduling;
```

When you enable packet-scheduling mode, the Packet Director application-specific integrated circuit (ASIC) schedules packet dispatches to compensate for transport delay differences. This preserves the interpacket gaps as the packets are distributed from the Packet Director ASIC to the Packet Forwarding Engine.

Whenever you change the configuration for packet-scheduling, the system stops all SFMs and FPCs and restarts them in the new mode.

**NOTE:** Packet scheduling is for M160 routers only.

## Configuring the Link Services PICs

The Multilink Protocol enables you to split, recombine, and sequence datagrams across multiple logical data links. The goal of multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the members.

The Links Services PIC supports the following Multilink Protocol encapsulation types at the logical unit level:

- Multilink Point-to-Point Protocol (MLPPP)
- Multilink Frame Relay (MLFR FRF.15)

The Link Services PIC also supports the Multilink Frame Relay UNI and NNI (MLFR FRF.16) encapsulation type at the physical interface level.

MLFR (FRF.16) is supported on a channelized interface, ls-*fpc/pic/port*:*channel*, which denotes a single MLFR (FRF.16) bundle. For MLFR (FRF.16), multiple links are combined to form one logical link. Packet fragmentation and reassembly occur on a per-virtual circuit (VC) basis. Each bundle can support multiple VCs. The physical connections must be E1, T1, channelized DS3 to DS1, channelized DS3 to DS0, channelized E1, channelized STM 1, or channelized IQ interfaces.

The default number of bundles per Link Services PIC is 16, ranging from ls-fpc/pic/port:0 to ls-fpc/pic/port:15.

To configure the number of bundles on a Link Services PIC, include the mlfr-uni-nni-bundles statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
mlfr-uni-nni-bundles number;
```

The maximum number of MLFR UNI NNI bundles each Link Services PIC can accommodate is 128. A link can associate with one link services bundle only. For more information, see the *JUNOS Network Interfaces Configuration Guide*.

**NOTE:** The Link Services PIC is not compatible with the M160 or T-series routing platforms.

### *Multiclass Extension to MLPPP (RFC 2686)*

This extension enables multiple classes of service using MLPPP. For more information, see RFC 2686, *The Multi-Class Extension to Multi-Link PPP*. The JUNOS software PPP implementation does not support the negotiation of address field compression and

protocol field compression PPP NCP options. The software always send a full 4-byte PPP header.

## Configuring the Idle Cell Format

ATM devices send idle cells to enable the receiving ATM interface to recognize the start of each new cell. The receiving ATM device does not act on the contents of idle cells and does not pass them up to the ATM layer in the ATM protocol stack.

By default, the idle cell format for ATM cells is (4 bytes): 0x00000000. For ATM 2 PICs only, you can configure the format of the idle cell header and payload bytes.

To configure the idle cell header to use the International Telecommunications Union (ITU-T) standard of 0x00000001, include the itu-t statement at the [edit chassis fpc *slot-number* pic *number* idle-cell-format] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number idle-cell-format]
itu-t;
```

On a TX Matrix platform, include the itu-t statement at the [edit chassis lcc *number* fpc *slot-number* pic *pic-number* idle-cell-format] hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number idle-cell-format]
itu-t;
```

By default, the payload pattern is cell payload (48 bytes). To configure the idle cell payload pattern, include the payload-pattern statement at the [edit chassis fpc *slot-number* pic *number* idle-cell-format] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number idle-cell-format]
payload-pattern payload-pattern-byte;
```

On a TX Matrix platform, include the payload-pattern statement at the [edit chassis lcc *number* fpc *slot-number* pic *pic-number* idle-cell-format] hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number idle-cell-format]
payload-pattern payload-pattern-byte;
```

The payload pattern byte can range from 0x00 through 0xff.

For information about the TX Matrix platform, see “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 779.

## Configuring an MTU Path Check for a Routing Instance

By default, the maximum transmission unit (MTU) check for routing instance is disabled on M-series routers (except the M320), and enabled for all T-series, and J-series routers.

**NOTE:** The MTU check is automatically present for interfaces belonging to the main router.

On M-series routers (except the M320 router) you can configure MTU path checks on the outgoing interface for unicast traffic routed on a virtual private network (VPN) routing and forwarding (VRF) routing instance. When you enable MTU check, the routing platform sends an Internet Control Message Protocol (ICMP) message when the size of a unicast packet traversing a VRF routing instance or virtual-router routing instance has exceeded the MTU size and when an IP packet is set to "do not fragment". The ICMP message uses the routing instance local address as its source address.

For an MTU check to work in a routing instance, you must include the vrf-mtu-check statement at the [edit chassis] hierarchy level and assign at least one interface containing an IP address to the routing instance.

To configure path MTU checks, do the following:

- Enabling MTU Check for a Routing Instance on page 769
- Assigning an IP Address to an Interface in the Routing Instance on page 769

### *Enabling MTU Check for a Routing Instance*

To enable MTU check for a routing instance, include the vrf-mtu-check statement at the [edit chassis] hierarchy level:

```
[edit chassis]
vrf-mtu-check;
```

### *Assigning an IP Address to an Interface in the Routing Instance*

To assign an IP address to an interface in the VRF or virtual-router routing instance, configure the local address for that routing instance. A local address is any IP address derived from an interface that is assigned to the routing instance.

To assign an interface to a routing instance, include the interface statement at the [edit routing-instances *routing-instance-name*] hierarchy level:

```
[edit routing-instances routing-instance-name]
interface interface-name;
```

To configure an IP address for a loopback interface, include the address statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet]
address address;
```

**NOTE:** If you are assigning Internet Protocol Security (IPSec) or generic routing encapsulation (GRE) tunnel interfaces without IP addresses in the routing instance, include a loopback interface to the routing instance. To do this, include the lo0.*n* option at the [edit routing-instances *routing-instance-name* interface] hierarchy level. *n* cannot be 0, because lo0.0 is reserved for the main router (and not appropriate for use with routing instances). Also, an IP address must be assigned to this loopback interface in order to work. To set an IP address for a loopback interface, include the address statement at the [edit interfaces lo0 unit *logical-unit-number* family inet] hierarchy level.

For more information about assigning an IP address to an interface in the VRF, see the *JUNOS VPNs Configuration Guide*.

## Configuring Redundancy

For routers that have multiple Routing Engines or these multiple switching control boards: Switching and Forwarding Modules (SFMs), System and Switch Boards (SSBs), Forwarding Engine Boards (FEBs), or Compact Forwarding Engine Boards (CFEBs), you can configure redundancy properties.

The following redundancy statements are available at the [edit chassis] hierarchy level:

```
redundancy {
    cfeb slot (always | preferred);
    failover {
        on-disk-failure
        on-loss-of-keepalives;
    }
    feb {
        redundancy-group group-name {
            feb slot-number (backup | primary);
            description description;
            no-auto-failover;
            }
        }
    graceful-switchover;
    keepalive-time seconds;
    routing-engine slot-number (master | backup | disabled);
    sfm slot-number (always | preferred);
    ssb slot-number (always | preferred);
}
```

For more information, see the *JUNOS High Availability Configuration Guide*.

## Configuring FPC to FEB Connectivity on M120 Routers

The M120 router supports six Forwarding Engine Boards (FEBs) and six Flexible PIC Concentrators (FPCs). The supported FPCs include:

- Two compact FPCs:

  - OC192 compact FPC (supported only on the D4 chip-based compact FPC)
  - 10-Gigabit Ethernet compact FPC
- Up to four Type 1, Type 2, or Type 3 FPCs

On the M120 router, you can map a connection between any FPC and any FEB. This capability allows you to configure resources for a chassis that contains empty slots, supporting configurations where the FPC and FEB pairs are not in slot order. You do not have to populate every empty slot position, but you must configure a FEB for every FPC.

If you do not want to map a connection between an FPC and a FEB, you must explicitly configure the FPC not to connect to the FEB. To do so, include the **none** option at the [edit chassis fpc-feb-connectivity fpc *number* feb] hierarchy level. If you do not configure FPC and FEB connectivity, it is automatically assigned in the following order: FPC 0 to FEB 0, FPC 1 to FEB 1, and so on.

For each FEB, you can map a maximum of two Type 1 FPCs or one Type 2, Type 3, or compact FPC.

The following restrictions apply when you configure FPC and FEB connectivity:

- When an FPC is configured not to connect to any FEB, interfaces on that FPC are not created.
- If a PIC comes online, but the FEB to which the FPC is configured to connect is not online, the physical interfaces for the PIC are not created. For example, PIC 1 on FPC 2 comes online. The configuration specifies that FPC 2 connects to FEB 3. If FEB 3 is not online at the time PIC 1 comes online, the physical interfaces corresponding to PIC 1 on FPC 2 are not created. If FEB 3 subsequently comes online, the physical interfaces are created.
- If a FEB is brought offline or removed, any interfaces on the FPCs connected to the FEB are deleted. If the FEB is subsequently brought back online, the interfaces are restored.
- FPCs and FEBs might reboot following a change in the FPC and FEB connectivity configuration. If an FPC connects to a different FEB as a result of the configuration change, the FPC is rebooted following the commit. As a result of the reboot, interfaces on the FPC are deleted.
- If a FEB connects to a different FPC or set of FPCs after a connectivity configuration change, the FEB is rebooted. The exception is if the FEB is already connected to one or two Type 1 FPCs and the change only results in the FEB being connected either to one additional or one fewer Type 1 FPC.

To configure a connection between an FPC and a FEB, include the **fpc-feb-connectivity** statement at the [edit chassis] hierarchy level:

```
[edit chassis]
fpc-feb-connectivity {
    fpc number feb (slot-number | none);
}
```

For fpc *number*, enter a value from 0 through 5. For feb *slot-number*, enter a value from 0 through 5 or none. The none option disconnects the FPC from the FEB.

To view the current FPC and FEB mapping and the status of each FPC and FEB, issue the show chassis fpc-feb-connectivity operational mode command. For more information, see the *JUNOS System Basics and Services Command Reference*.

**NOTE:** FPC-to-FEB connectivity is supported only on the M120 router.

### *Example: Configuring FPC to FEB Connectivity on the M120 Router*

In this example, FPC 3 is already mapped to FEB 3 by default. You are also mapping a connection between FPC 2 and FEB 3.

```
[edit chassis]
fpc-feb-connectivity {
   fpc 2 feb 3;
}
```

However, this configuration results in a mismatch between the FPC type and the FEB type. For example, FPC 3 is not a Type 1 FPC. You can map only one FPC that is not a Type 1 FPC to a FEB. Use the fpc-feb-connectivity statement to explicitly disconnect FPC 3 from FEB 3. To do so, include the none option at the [edit chassis fpc-feb-connectivity fpc *number* feb] hierarchy level:

```
[edit chassis]
fpc-feb-connectivity {
   fpc 2 feb 3;
   fpc 3 feb none;
}
```

## Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors

When a hard disk error occurs, a Routing Engine might enter a state in which it responds to local pings and interfaces remain up, but no other processes are responding.

To enable routers with a single Routing Engine (such as the M7i and M10i routers) to recover from this situation, you can configure the Routing Engine either to halt or to reboot when its hard disk fails. Include the disk-failure-action (halt | reboot) statement at the [edit chassis routing-engine on-disk-failure] hierarchy level:

```
[edit chassis routing-engine]
on-disk-failure {
disk-failure-action (halt | reboot);
}
```

Use halt to configure the Routing Engine to halt when the hard disk fails. Use reboot to configure the Routing Engine to reboot when the hard disk fails. For M7i and M10i routers, we recommend that you configure the Routing Engine to halt instead of rebooting when the hard disk fails.

You can also include the on-disk-failure statement on routers with dual Routing Engines, but we recommend that you configure the backup Routing Engine to assume mastership automatically when it detects a hard disk error on the master Routing Engine. To enable this feature, include the on-disk-failure statement at the [edit chassis redundancy failover] hierarchy level. For information about this statement, see the *JUNOS High Availability Configuration Guide*.

## Configuring the CONFIG Button

On J-series Services Routers, if the current configuration fails, you can load a rescue configuration or the factory default configuration by pressing the CONFIG (Reset) button:

- Rescue configuration—When you press and quickly release the CONFIG button, the configuration LED blinks green and the rescue configuration is loaded and committed. The rescue configuration is user defined and must be set previously for this operation to be successful.
- Factory defaults—When you hold the CONFIG button for more than 15 seconds, the configuration LED blinks red and the router is set back to the factory default configuration.

**CAUTION:** When you set the router back to the factory default configuration, the current committed configuration and all previous revisions of the router's configuration are deleted.

To limit how the CONFIG button resets a router configuration, include one or both of the following statements at the [edit chassis] hierarchy level:

```
[edit chassis]
config-button {
    no-clear;
    no-rescue;
}
```

no-clear—Prevents resetting the router to the factory default configuration. You can still press and quickly release the button to reset to the rescue configuration (if one was set previously).

no-rescue—Prevents resetting the router to the rescue configuration. You can still press and hold the button for more than 15 seconds to reset to the factory default configuration.

When both the no-clear and no-rescue statements are present, the CONFIG button does not reset to either configuration.

## Configuring Larger Delay Buffers

By default, T1, E1, and *N*xDS0 interfaces configured on Channelized IQ PICs are limited to 100,000 microseconds of delay buffer. (The default average packet size on the IQ PIC is 40 bytes.) For these interfaces, it might be necessary to configure a larger buffer size to prevent congestion and packet dropping.

To ensure traffic is queued and transmitted properly, you can configure a buffer size larger than the default maximum. Include the q-pic-large-buffer large-scale statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
q-pic-large-buffer {
    large-scale;
}
```

This statement sets the maximum buffer size. (See Table 57 on page 774.)

**Table 57: Maximum Delay Buffer with q-pic-large-buffer Statement Enabled**

| Platform, PIC, or Interface Type | Maximum Buffer Size |
|---|---|
| **With Large Buffer Sizes Not Enabled** | |
| T-series and M320 | 50,000 microseconds |
| Other M-series | 200,000 microseconds |
| IQ PICs on all platforms | 100,000 microseconds |
| Channelized T1/E1 interface on J-series Services Routers | 400,000 microseconds |
| **With Large Buffer Sizes Enabled** | |
| Channelized T3 and channelized OC3 DLCIs—Maximum sizes vary by shaping rate: | |
| With shaping rate from 64,000 through 255,999 bps | 4,000,000 microseconds |
| With shaping rate from 256,000 through 511,999 bps | 2,000,000 microseconds |
| With shaping rate from 512,000 through 1,023,999 bps | 1,000,000 microseconds |
| With shaping rate from 1,024,000 through 2,048,000 bps | 500,000 microseconds |
| With shaping rate from 2,048,001 bps through 10 Mbps | 400,000 microseconds |
| With shaping rate from 10,000,001 bps through 20 Mbps | 300,000 microseconds |
| With shaping rate from 20,000,001 bps through 30 Mbps | 200,000 microseconds |

**Table 57: Maximum Delay Buffer with q-pic-large-buffer Statement Enabled** *(continued)*

| Platform, PIC, or Interface Type | Maximum Buffer Size |
|---|---|
| With shaping rate from 30,000,001 bps through 40 Mbps | 150,000 microseconds |
| With shaping rate up to 40,000,001 bps or higher | 100,000 microseconds |
| *N*xDS0 IQ Interfaces—Maximum sizes vary by channel size: | |
| 1xDSO through 3xDS0 | 4,000,000 microseconds |
| 4xDSO through 7xDS0 | 2,000,000 microseconds |
| 8xDSO through 15xDS0 | 1,000,000 microseconds |
| 16xDSO through 32xDS0 | 500,000 microseconds |
| Other IQ interfaces | 500,000 microseconds |

For information on configuring the buffer size, see the *JUNOS Class of Service Configuration Guide*.

## Configuring an Entry-Level M320 Router

An M320 router can include an entry-level configuration with a minimum number of SIBs and PEMs. With this configuration, the router may have fewer than four SIBs or four PEMs.

To prevent unwanted alarms from occurring with this entry-level configuration, include the pem minimum and sib minimum statements at the [edit chassis] hierarchy level:

```
[edit chassis]
pem {
    minimum number;
}
sib {
    minimum number;
}
```

minimum *number* can be 0 through 3. With this configuration, SIB absent or PEM absent alarms are generated only if the SIB or PEM count falls below the minimum specified. For example, set this number to 2 for an entry-level configuration with 2 Switch Interface Boards and 2 Power Entry Modules.

## Configuring the uPIM Mode on J-series Routers

The 6-port, 8-port, and 16-port Gigabit Ethernet uPIMs used on the J-series routers (J2320, J2350, J4350, and J6350) support Layer 2 switching and can forward traffic

at both Layer 2 (switching) and Layer 3 (routing). You can configure a uPIM to run in either routing mode (the default) or switching mode.

Routing mode provides the standard routing services. Switching mode allows traffic forwarding at both Layer 2 and Layer 3. At Layer 2, a uPIM can switch intra-LAN traffic from one LAN host to another, such as from one port on a uPIM to another on the same uPIM. At Layer 3, a uPIM can route traffic to WAN interfaces and other PIMs present on the chassis.

To configure the PIM mode, include the following statements at the [edit chassis fpc] hierarchy level:

```
[edit chassis]
fpc fpc-slot {
    pic pim-slot {
        ethernet {
            pic-mode (switching | routing);
        }
    }
}
```

### Setting J-Series PIMs Offline

On J-series routers, the system monitors the PIMs and verifies that a newly inserted PIM falls within the power capacity of the chassis. PIMs that fall outside of acceptable power ranges can be taken offline or disabled for power management purposes.

This operation differs from the power-off option used on non-J-series products.

To take a PIM offline, include the offline statement at the [edit chassis fpc *slot-number*] hierarchy level:

```
[edit chassis fpc slot-number]
offline;
```

### Disabling Power Management on the J-series Chassis

Instead of setting a PIM offline, the power management feature on a chassis can be disabled. The disable-power-management statement disables power management on the chassis and, when used, causes any PIMs disabled due to exceeding chassis power limits to come online.

It is important to consider power management carefully before enabling disabled PIMs. If the PIMs have been disabled because they exceeded power limits, they should not be enabled.

To disable power on the J-series chassis, include the disable-power-management statement at the [edit chassis] hierarchy level:

```
[edit chassis]
disable-power-management;
```

## Configuring the IP and Ethernet Services Mode in MX-series Routers

MX-series Ethernet services routers can be configured to run in IP Services mode or in Ethernet Services mode. The default IP Services mode provides complete functionality, while the Ethernet Services mode only provides support for Layer 2.5 functions.

Operating in Ethernet Services mode restricts certain BGP protocol functions and does not support Layer 3 VPN, unicast RPF, and source and destination class usage (SCU and DCU) functions. In addition, the number of externally configured filter terms are restricted to 64K. The details of Layer 2.5 support for Ethernet Services are shown in Table 58 on page 777.

To configure the network services mode of an MX-series router, include the network-services statement with the appropriate option at the [edit chassis] hierarchy level:

```
[edit chassis]
network-services (ethernet | ip);
```

If DPCs in Ethernet Services mode are up and running, the system cannot be set to IP services mode. You must set any Ethernet mode DPCs offline before switching to IP Services mode.

If you use VPLS-PE, then network-services must be set to ethernet since it uses the X-DPC cards. The X-DPC cards only support BGP family l2vpn, not the other BGP families. Use edit chassis to configure the MX-series network services mode; use set to enter commands.

## Restrictions on JUNOS Features for MX-series Routers

The following features contain restrictions when running in Ethernet Services mode.

**Table 58: Restricted Software Features in Ethernet Services Mode**

| Software Feature | Restriction in Ethernet Services Mode |
|---|---|
| BGP | ■ BGP allows only family L2 VPN to provide IP control plane support.<br>■ Data plane support applies only for Ethernet and MPLS.<br>■ BGP in Ethernet Services mode does not support inet, inet6, inet-vpn and inet-6vpn |
| L3VPN | Layer 3 VPN is not available in Ethernet Services mode. |
| Unicast RPF | Unicast reverse-path forwarding is disabled when running Ethernet Services mode. |
| Source and destination class usage (SCU and DCU) | Source and Destination Class Usage is disabled when running Ethernet Services mode. |

**Table 58: Restricted Software Features in Ethernet Services Mode** *(continued)*

| Software Feature | Restriction in Ethernet Services Mode |
|---|---|
| Filter terms | When running Ethernet Services mode, the number of externally configured filter terms is restricted to 64 KB. |

## Configuring J-series Services Router Switching Interfaces

In access switching mode, only one physical interface is configured for the entire Gigabit Ethernet uPIM. The single physical interface serves as a Virtual Router Interface (VRI). Configuration of the physical port characteristics is done under the single physical interface.

To configure Gigabit Ethernet uPIM physical Ethernet interface properties, include the switch-port-parameters statement at the [edit interfaces [ge-*pim*/0/0] hierarchy level:

```
[edit interfaces ge-pim /0/0]
{
   switch-port port-number {
      (auto-negotiation | no-auto-negotiation);
      speed (10m | 100m | 1g);
      link-mode (full-duplex | half-duplex);
   }
}
```

### *Example: Configuring J-series Services Router Switching Interfaces*

Configure a single physical interface for the uPIM and set the port parameters for port 0 and port 1:

```
[edit interfaces]
ge-2/0/0 {
   {
      switch-port 0 {
         no-auto-negotiation;
         1g;
         link-mode full-duplex;
      }
      port 1 {
         no-auto-negotiation;
         10m;
         link-mode half-duplex;
      }
   }
}
```

## TX Matrix Platform and T640 Routing Node Configuration Guidelines

To configure a T640 routing node that is connected to a TX Matrix platform within a routing matrix, include the following statements at the [edit chassis lcc *number*] hierarchy level:

```
[edit chassis lcc number]
fpc slot-number {
    pic pic-number {
        atm-cell-relay-accumulation;
        atm-l2circuit-mode (cell | aal5 | trunk trunk);
        framing (sdh | sonet);
        idle-cell-format {
            itu-t;
            payload-pattern payload-pattern-byte;
        }
        max-queues-per-interface (8 | 4);
        no-concatenate;
    }
}
offline;
online-expected;
```

This section includes only configuration guidelines that are unique to the TX Matrix platform and its connected T640 routing nodes. The remaining statements are explained separately in this chapter.

This section contains the following topics:

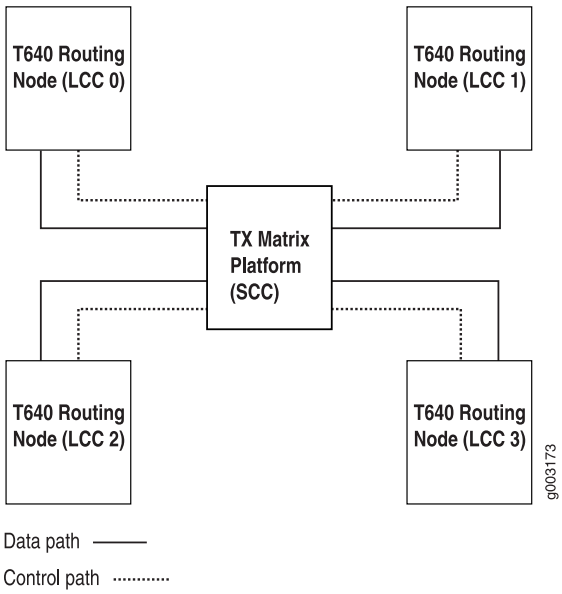


For a complete description of the TX Matrix routing platform see the “Routing Matrix” chapter of the *JUNOS Feature Guide*.

### *Routing Matrix Overview*

A routing matrix is a multichassis architecture that consists of a TX Matrix platform and from one to four T640 routing nodes. From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix platform controls all the T640 routing nodes in the routing matrix, as shown in Figure 10 on page 780.

**Figure 10: Routing Matrix**




You configure and manage the TX Matrix platform and its T640 routing nodes in the routing matrix through the CLI on the TX Matrix platform. This means that the configuration file on the TX Matrix platform is used for the entire routing matrix.

Because all configuration, troubleshooting, and monitoring is performed through the TX Matrix platform, we do not recommend accessing its T640 routing nodes directly (through the console port or management Ethernet [fxp0]). If you do, the following messages appear when you first start the CLI through a T640 routing node:

```
% cli
warning: This chassis is a Line Card Chassis (LCC) in a multichassis system.
warning: Use of interactive commands should be limited to debugging.
warning: Normal CLI access is provided by the Switch Card Chassis (SCC).
warning: Use 'request routing-engine login scc' to log into the SCC.
{master}
```

These messages appear because any configuration you commit on a T640 routing node is not propagated to the TX Matrix platform or other T640 routing nodes. For details, see “Committing Configurations” on page 781.

## *Running Different JUNOS Software Releases*

On a routing matrix, if you elect to run different JUNOS software releases on the TX Matrix platform and T640 Routing Engines, a change in Routing Engine mastership can cause one or all T640 routing nodes to be logically disconnected from the TX Matrix platform. For more information, see the *JUNOS High Availability Configuration Guide*.

**NOTE:** The routing matrix supports Release 7.0 and later versions of the JUNOS software. All the master Routing Engines on the routing matrix must use the same software version. For information about hardware and software requirements, see the *TX Matrix Platform Hardware Guide*.

### *Software Upgrades and Reinstallation*

By default, when you upgrade or reinstall software on the TX Matrix platform, the new software image is distributed to the connected T640 routing nodes. Software installed on a primary TX Matrix platform is distributed to all connected primary T640 nodes and the backup is distributed to all connected backup nodes.

### *Rebooting Process*

When you reboot the TX Matrix platform master Routing Engine, all the master Routing Engines in the connected T640 routing nodes reboot. In addition, you can selectively reboot the master Routing Engine or any of the connected T640 routing nodes.

### *Committing Configurations*

In a routing matrix, all configuration must be performed on the TX Matrix platform. Any configuration you commit on a T640 routing node is not propagated to the TX Matrix platform or other T640 routing nodes. Only configuration changes you commit on the TX Matrix platform are propagated to all T640 routing nodes. A commit on a TX Matrix platform overrides any changes you commit on a T640 routing node.

If you issue the commit command, you commit the configuration to all the master Routing Engines in the routing matrix.

```
user@host# commit
scc-re0:
configuration check succeeds
lcc0-re0:
commit complete
lcc1-re0:
commit complete
scc-re0:
commit complete
```

**NOTE:** If a commit operation fails on any node, then the commit operation is not completed for the entire TX Matrix platform.

If you issue the commit synchronize command on the TX Matrix platform, you commit the configuration to all the master and backup Routing Engines in the routing matrix.

```
user@host# commit synchronize
scc-re0:
configuration check succeeds
```

```
lcc0-re1:
commit complete
lcc0-re0:
commit complete
lcc1-re1:
commit complete
lcc1-re0:
commit complete
scc-re1:
commit complete
scc-re0:
commit complete
```

### *Configuring a T640 Routing Node Within a Routing Matrix*

A routing matrix supports the same chassis configuration statements as a standalone routing platform (except ce1, ct3, mlfr-uni-nni-bundles, sparse-dlcis, and vtmapping). By including the lcc statement at the [edit chassis] hierarchy level, you configure PIC-specific features, such as framing, on specific T640 routing nodes. In addition, a routing matrix has two more chassis configuration statements, online-expected and offline.

To configure a T640 routing node that is connected to a TX Matrix platform, include the lcc statement at the [edit chassis] hierarchy level:

```
[edit chassis]
lcc number;
```

*number* can be 0 through 3.

To configure a T640 routing node within a routing matrix, include the following statements at the [edit chassis lcc *number*] hierarchy level:

```
[edit chassis lcc number]
fpc slot-number { # Use the hardware FPC slot number
pic pic-number {
   atm-cell-relay-accumulation;
   atm-l2circuit-mode (cell | aal5 | trunk trunk);
   framing (sdh | sonet);
   idle-cell-format {
      itu-t;
      payload-pattern payload-pattern-byte;
   }
   max-queues-per-interface (8 | 4);
   no-concatenate;
}
offline;
online-expected;
```

**NOTE:** For the FPC slot number, specify the actual hardware slot number (numbered 0 through 7) as labeled on the T640 routing node chassis. Do not use the corresponding software FPC number shown in the Table 59 on page 783.

For information about how to configure the online-expected and offline configuration statements, see “Configuring the Online Expected Alarm” on page 785.

### Chassis and Interface Names

The output from some CLI commands uses the terms SCC and scc (for *switch-card chassis*) to refer to the TX Matrix platform. Similarly the terms LCC, and lcc as a prefix (for *line-card chassis*) refer to a T640 routing node in a routing matrix.

T640 routing noticed are assigned LCC index numbers, 0 through 3, depending on the hardware setup to the TX Matrix platform. A routing matrix can have up to four T640 routing nodes, and each T640 routing node has up to eight FPCs. Therefore, the routing matrix can have up to 32 FPCs (0 through 31). The FPCs are configured at the [edit chassis lcc *number*] hierarchy level.

In the JUNOS CLI, an interface name has the following format:

type-*fpc/pic/port*

When you specify the FPC number, the JUNOS software determines which T640 routing node contains the specified FPC based on the following assignment:

- On LCC 0, FPC hardware slots 0 through 7 correspond to FPC software numbers 0 through 7.
- On LCC 1, FPC hardware slots 0 through 7 correspond to FPC software numbers 8 through 15.
- On LCC 2, FPC hardware slots 0 through 7 correspond to FPC software numbers 16 through 23.
- On LCC 3, FPC hardware slots 0 through 7 correspond to FPC software numbers 24 through 31.

To convert FPC numbers in the T640 routing nodes to the correct FPC in a routing matrix, use the conversion chart shown in Table 59 on page 783. You can use the converted FPC number to configure the interfaces on the TX Matrix platform in your routing matrix.

**Table 59: T640 to Routing Matrix FPC Conversion Chart**

| FPC Numbering | T640 Routing Nodes | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **LCC 0** | | | | | | | |
| **T640 FPC Slots** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Routing Matrix FPC Slots Equivalent** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | **LCC 1** | | | | | | | |
| **T640 FPC Slots** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Routing Matrix FPC Slots Equivalent** | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

**Table 59: T640 to Routing Matrix FPC Conversion Chart** *(continued)*

| FPC Numbering | T640 Routing Nodes | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **LCC 2** | | | | | | | |
| **T640 FPC Slots** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Routing Matrix FPC Slots Equivalent** | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| | **LCC 3** | | | | | | | |
| **T640 FPC Slots** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Routing Matrix FPC Slots Equivalent** | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |

Some examples include:

- In a routing matrix that contains lcc 0 through lcc 2, so-20/0/1 refers to FPC slot 4 of lcc 2.
- If you have a Gigabit Ethernet interface installed in FPC slot 7, PIC slot 0, port 0 of T640 routing node LCC 3, you can configure this interface on the TX Matrix platform by including the ge-31/0/0 statement at the [edit interfaces] hierarchy level.

```
[edit]
interfaces {
   ge-31/0/0 {
      unit 0 {
         family inet {
            address ip-address;
         }
      }
   }
}
```

For more information about the interface-naming conventions for a routing matrix, see the *JUNOS Network Interfaces Configuration Guide*.

## *Upgrading Switch Interface Boards*

The JUNOS software does not support mixed mode operation of switch interface boards (SIBs). To successfully upgrade 1.0 SIBs to 2.0 SIBs in a TX Matrix environment, you must force all newly installed 2.0 SIBs to operate in 1.0 mode until the upgrade is complete.

To configure the TX Matrix to support a SIB upgrade, include the fabric upgrade-mode statement at the [edit chassis] hierarchy level and commit the changes to update the configuration. Configuration changes that you commit on the TX Matrix platform are propagated to all T640 routing nodes.

```
[edit chassis]
user@host# set chassis fabric upgrade-mode
```

```
user@host# commit
```

The fabric upgrade-mode statement instructs the newly installed 2.0 boards to operate in 1.0 mode. When all 1.0 boards have been replaced by 2.0 boards, remove the fabric upgrade-mode statement from the configuration hierarchy, and commit the changes again.

```
[edit chassis]
user@host# delete chassis fabric upgrade-mode
user@host# commit
```

Use the request chassis sib (offline | online) command sequence to power cycle the newly installed 2.0 SIBs.

```
user@host> request chassis sib offline slot slot-number
user@host> request chassis sib online slot slot-number
```

As the system discovers each new board, the 2.0 ASIC enables 2.0 features, and the upgrade is complete.

### Downgrading Switch Interface Boards

To downgrade your 2.0 SIBs to 1.0 SIBs, follow the upgrade procedure. When you replace the first 2.0 SIB with a 1.0 SIB, the system operates in a downgraded 1.0 mode until all 2.0 SIBs are replaced, and the newly installed 1.0 SIBs are power cycled using a request chassis sib (offline | online) command sequence.

**NOTE:** The TX Matrix switch fabric supports 2.0 SIBs for enabling Gigabit FPC-4 and Type 4 PICs. Gigabit FPC-4 devices are not compatible with 1.0 SIBs. Therefore, if you are planning to downgrade from 2.0 SIBs to 1.0 SIBs, you must take all Gigabit FPC-4 devices offline to ensure that the link between the new SIBs and the FPC does not fail.

## *Configuring the Online Expected Alarm*

By default, the JUNOS software allows all the T640 routing nodes in the routing matrix to come online. The JUNOS software also allows you to configure all the T640 routing nodes so that if they do not come online, an alarm is sent by the TX Matrix platform.

To configure this alarm, include the online-expected statement at the [edit chassis lcc *number*] hierarchy level:

```
[edit chassis lcc number]
online-expected;
```

If you do not want a T640 routing node to be part of the routing matrix, you can configure it to be offline. This is useful when you are performing maintenance on a T640 routing node. When the T640 routing is ready to come back online, delete the offline configuration statement.

To configure a T640 routing so that it is offline, include the offline statement at the [edit chassis lcc *number*] hierarchy level:

```
[edit chassis lcc number]
offline;
```

**NOTE:** If you do not configure the online-expected or offline statement, any T640 routing node that is part of the routing matrix is allowed to come online. However, if a T640 routing node does not come online, the TX Matrix platform does not generate an alarm.

### *Creating Configuration Groups*

For routers that include two Routing Engines, you can specify two special group names—re0 and re1. These two special group names apply to the Routing Engines in slots 0 and 1 of the TX Matrix platform. In addition, the routing matrix supports group names for the Routing Engines for each T640 routing node: lcc *n*-re0 and lcc *n*-re1. *n* identifies a T640 routing node from 0 through 3. For more information about configuration groups, see the *JUNOS CLI User Guide*.

### *Configuring System Log Messages*

You configure the T640 routing nodes to forward their system log messages to the TX Matrix platform at the [edit system syslog host scc-master] hierarchy level. For information about how to configure system log messages in a routing matrix, see "Configuring System Log Messages" on page 109 and "Configuring System Logging for a Routing Matrix" on page 132.

Chapter 25

# Summary of Router Chassis Configuration Statements

The following sections explain each of the chassis configuration statements. The statements are organized alphabetically.

## adaptive-services

**Syntax**
```
adaptive-services {
   (layer-2 | layer-3);
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Enable a service package on adaptive services interfaces.

**Options** The statements are explained separately.

**Usage Guidelines** See "Configuring Service Packages on Adaptive Services Interfaces" on page 753.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** *JUNOS Services Interfaces Configuration Guide* and *JUNOS Feature Guide*

## aggregate-ports

**Syntax** aggregate-ports;

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced in JUNOS Release 8.1.

**Description** For T-series routers only, specify OC768-over-OC192 mode on the 4-port OC192C PIC. Four OC192 links are aggregated into one OC768 link with one logical interface.

**Usage Guidelines** See *JUNOS Interfaces Network Operations Guide*.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## aggregated-devices

**Syntax**

```
aggregated-devices {
    ethernet {
        device-count number;
        lacp {
            link-protection {
                non-revertive;
            }
            system-priority;
        }
    }
    sonet {
        device-count number;
    }
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 7.4.
Support for LACP link protection and system priority introduced in JUNOS Release 9.3.

**Description** Configure properties for aggregated devices on the router.

**Options** The statements are explained separately in this chapter.

**Usage Guidelines** See “Configuring Aggregated Devices” on page 712.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## alarm

**Syntax**

```
alarm {
    interface-type {
        alarm-name (red | yellow | ignore);
    }
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the chassis alarms and whether they trigger a red or yellow alarm, or whether they are ignored. Red alarm conditions light the RED ALARM LED on the router's craft interface and trigger an audible alarm if one is connected to the contact on the craft interface. Yellow alarm conditions light the YELLOW ALARM LED on the router's craft interface and trigger an audible alarm if one is connected to the craft interface.

To configure more than one alarm, include multiple *alarm-name* lines.

**Options** *alarm-name*—Alarm condition. For a list of conditions, see Table 44 on page 718.

*ignore*—The specified alarm condition does not set off any alarm.

*interface-type*—Type of interface on which you are configuring the alarm. It can be one of the following: atm, ethernet, sonet, or t3.

red—The specified alarm condition sets off a red alarm.

yellow—The specified alarm condition sets off a yellow alarm.

**Usage Guidelines** See "Chassis Conditions That Trigger Alarms" on page 719.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## atm-cell-relay-accumulation

**Syntax** atm-cell-relay-accumulation;

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure an Asynchronous Transfer Mode (ATM) Physical Interface Card (PIC) in cell-relay accumulation mode.

**Usage Guidelines** See "Configuring ATM Cell-Relay Accumulation Mode on an ATM1 PIC" on page 714.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## atm-l2circuit-mode

**Syntax** atm-l2circuit-mode (cell | aal5 | trunk *trunk*);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the ATM2 intelligent queuing (IQ) Layer 2 circuit transport mode.

**Default** aal5

**Options** aal5—Tunnel a stream of ATM cells encoded with ATM Adaptation Layer (AAL5) over an IP Multiprotocol Label Switching (MPLS) backbone.

cell—Tunnel a stream of ATM cells over an IP MPLS backbone.

trunk *trunk*—Transport ATM cells over an MPLS core network that is implemented on some other vendor switches. Trunk mode can be UNI or NNI.

**NOTE:** To determine which vendors support Layer 2 circuit trunk mode, contact Juniper Networks Customer Support.

**Usage Guidelines** See "Configuring ATM2 Intelligent Queuing Layer 2 Circuit Transport Mode" on page 763.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## bandwidth

**Syntax** bandwidth (1g | 10g);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *number* tunnel-services]

**Release Information** Statement introduced in JUNOS Release 8.2.

**Description** On the MX-series Ethernet Services routers only, specify the amount of bandwidth to reserve for tunnel services.

**Options**

1g—Specify a bandwidth of 1 Gbps on the Packet Forwarding Engine connected to a Gigabit Ethernet 40-port Dense Port Concentrator (DPC).

10g—Specify a bandwidth of 10 Gbps on the Packet Forwarding Engine connected to 10-Gigabit Ethernet 4-port DPC.

**NOTE:** If you specify a bandwidth that is not compatible with the type of DPC and Packet Forwarding Engine, tunnel services are not activated. For example, you cannot specify a bandwidth of 1 Gbps for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.

**Usage Guidelines** See "Configuring Tunnel Interfaces on MX-Series Ethernet Services Routers" on page 764.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## ce1

**Syntax**
```
ce1 {
   e1 port-number {
      channel-group group-number timeslots slot-number;
   }
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure channelized E1 port and channel specifications.

**Options** *port-number*—Any valid E1 port number on the host system.

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See "Configuring Channelized E1 Naming" on page 761.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## channel-group

**Syntax** channel-group *group-number;*

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* ce1 e1 *port-number*],
[edit chassis fpc *slot-number* pic *pic-number* ct3 port *port-number* t1 *link-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the DS0 channel number.

**Options** *group-number*—DS0 channel group.
**Range:** 0 through 7 for DS0 naming, and 0 through 23 for E1 naming.

**Usage Guidelines** See "Configuring Channelized DS3-to-DS0 Naming" on page 758 and "Configuring Channelized E1 Naming" on page 761.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## chassis

**Syntax** chassis { ... }

**Hierarchy Level** [edit]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure router chassis properties.

**Usage Guidelines** See “Router Chassis Configuration Guidelines” on page 707.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## config-button

**Syntax**
```
config-button {
    no-clear;
    no-rescue;
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** (J-series Services Routers only) Configure the CONFIG button on the router to prevent resetting the router to the factory default or rescue configuration.

**Options** no-clear—Prevent resetting the router to the factory default configuration. You can still press and quickly release the button to reset to the rescue configuration (if one was set previously).

no-rescue—Prevent resetting the router to the rescue configuration. You can still press and hold the button for more than 15 seconds to reset to the factory default configuration.

When both the no-clear and no-rescue statements are present, the CONFIG button is deactivated for all types of reset.

**Usage Guidelines** See “Configuring the CONFIG Button” on page 773.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## craft-lockout

**Syntax** craft-lockout;

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in JUNOS Release 8.1.

**Description** Disable the physical operation of the craft interface front panel.

**Usage Guidelines** See "Disabling Physical Operation of the Craft Interface" on page 752.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## ct3

**Syntax**
```
ct3 {
   port port-number {
      t1 link-number {
         channel-group group-number timeslots slot-number;
      }
   }
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure channelized T3 port and channel specifications.

**Options** port *port-number*—Any valid T3 port number on the host system.

t1 *link-number*—T1 link.
**Range:** 0 through 27

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See "Configuring Channelized DS3-to-DS0 Naming" on page 758.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## device-count

**Syntax** device-count *number*;

**Hierarchy Level** [edit chassis aggregated-devices ethernet]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the number of aggregated logical devices available to the router.

**Usage Guidelines** See “Configuring Aggregated Devices” on page 712.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## disk-failure-action

**Syntax** disk-failure-action (halt | reboot);

**Hierarchy Level** [edit chassis routing-engine on-disk-failure]

**Release Information** Statement introduced in JUNOS Release 9.0.

**Description** On M7i and M10i routers only, configure the Routing Engine to halt or reboot when the Routing Engine hard disk fails.

**Options** halt—Specify the Routing Engine to halt.

reboot—Specify the Routing Engine to reboot.

**Usage Guidelines** See “Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors” on page 772.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## e1

**Syntax**
```
e1 port-number {
    channel-group group-number timeslots slot-number;
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* ce1]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the channelized E1 port number on the PIC.

Range: 0 through 9

**Usage Guidelines** See "Configuring Channelized E1 Naming" on page 761.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## ethernet

**Syntax**
```
ethernet {
    device-count number;
    lacp {
        link-protection {
            non-revertive;
        }
        system-priority;
    }
}
```

**Hierarchy Level** [edit chassis aggregated-devices]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure properties for Ethernet aggregated devices on the router.

**Usage Guidelines** See "Configuring Aggregated Devices" on page 712.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## fabric upgrade-mode

**Syntax**
```
fabric {
    upgrade-mode;
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in JUNOS Release 7.5.

**Description** Configure upgrade mode for SIBs and forces them to operate in the same mode until the upgrade is complete.

**Usage Guidelines** See "TX Matrix Platform and T640 Routing Node Configuration Guidelines" on page 779.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## fpc

See the following topics:

- fpc (M320, T320, T640 Routing Platforms) on page 799
- fpc (MX-Series Ethernet Services Routers) on page 800
- fpc (TX Matrix Platform) on page 801

### *fpc (M320, T320, T640 Routing Platforms)*

**Syntax**

```
fpc slot-number {
   pic pic-number {
      ce1 {
         e1 port-number {
            channel-group group-number timeslots slot-number;
         }
      }
      ct3 {
         port port-number {
            t1 link-number {
               channel-group group-number timeslots slot-number;
            }
         }
      }
      framing (sdh | sonet);
      idle-cell-format {
         itu-t;
         payload-pattern payload-pattern-byte;
      }
      max-queues-per-interface (8 | 4);
      no-concatenate;
      q-pic-large-buffer <large-scale | small-scale>;
   }
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure properties for the PICs in individual Flexible PIC Concentrators (FPCs).

**Options** *slot-number*—Slot number in which the FPC is installed.
**Range:** 0 through 7

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Configuring SONET/SDH Framing” on page 754 and “Configuring Channelized PIC Operation” on page 757.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## *fpc (MX-Series Ethernet Services Routers)*

**Syntax**

```
fpc slot-number {
   pic number {
      port-mirror-instance pm-instance-name-pic-level;
      tunnel-services {
         bandwidth (1g | 10g)
      }
   }
   port-mirror-instance pm-instance-name-fpc-level;
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in JUNOS Release 8.2.
port-mirror-instance option introduced in JUNOS Release 9.3.

**Description** On MX-series Ethernet Services Routers only, configure properties for the DPC and corresponding Packet Forwarding Engines to create tunnel interfaces.

Configure a port-mirroring instance for the DPC and its corresponding Packet Forwarding Engines.

**Options** *slot-number*—Specify the slot number of the DPC.
**Range:** 0 through 11

pic *number*—Specify the number of the Packet Forwarding Engine. Each DPC includes four Packet Forwarding Engines.
**Range:** 0 through 4

port-instance-name—Associate a port-mirroring instance with the DPC and its corresponding PICs. The port-mirroring instance is configured under the [edit forwarding-options port-mirroring] hierarchy level.

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Configuring Tunnel Interfaces on MX-Series Ethernet Services Routers” on page 764 and “Configuring Port Mirroring Instances on MX-series Routers” on page 715.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## *fpc (TX Matrix Platform)*

**Syntax**

```
fpc slot-number {
    pic pic-number {
        atm-cell-relay-accumulation;
        atm-l2circuit-mode (cell | aal5 | trunk trunk);
        framing (sdh | sonet);
        idle-cell-format {
            itu-t;
            payload-pattern payload-pattern-byte;
        }
        max-queues-per-interface (8 | 4);
        no-concatenate;
        q-pic-large-buffer <large-scale | small-scale>;
    }
}
```

**Hierarchy Level** [edit chassis lcc *number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** On a TX Matrix platform, configure properties for the PICs in individual FPCs.

**Options** *slot-number*—Slot number in which the FPC is installed.
**Range:** 0 through 7

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See "Configuring SONET/SDH Framing" on page 754 and "Chassis and Interface Names" on page 783.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## fpc-feb-connectivity

**Syntax**
```
fpc-feb-connectivity {
    fpc number feb (slot-number | none);
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in JUNOS Release 8.0.

**Description** On the M120 router only, configure a connection between any Flexible PIC Concentrator (FPC) and any Forwarding Engine Board (FEB).

**Options** fpc *number*—Specify the FPC slot number.
**Range:** 0 through 5

feb *slot-number*—Specify the FEB slot number.
**Range:** : 0 through 5

none—Disconnects the FPC from the FEB.

**Usage Guidelines** See "Configuring FPC to FEB Connectivity on M120 Routers" on page 770.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## framing

**Syntax** framing (sdh | sonet);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number*] (Routing Matrix)

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** On SONET/SDH PICs only, configure the framing type.

**Default** sonet

**Options** sdh—SDH framing.

sonet—SONET framing.

**Usage Guidelines** See "Configuring SONET/SDH Framing" on page 754.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## idle-cell-format

**Syntax**
```
idle-cell-format {
    itu-t;
    payload-pattern payload-pattern-byte;
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* idle-cell-format],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number* idle-cell-format]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For ATM2 PICs only, configure the format of the idle cell header and payload bytes.

**Options** itu-t—Configure the idle cell header to use the International Telecommunications Union (ITU-T) standard of 0x00000001.
**Default:** (4 bytes): 0x00000000

*payload-pattern-byte*—Configure the idle cell payload pattern. The payload pattern byte can range from 0x00 through 0xff.
**Default:** cell payload (48 bytes)

**Usage Guidelines** See "Configuring the Idle Cell Format" on page 768.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## lacp

**Syntax**
```
lacp {
    link-protection {
        non-revertive;
    }
    system-priority priority;
}
```

**Hierarchy Level** [edit chassis aggregated-devices ethernet]

**Release Information** Statement introduced in JUNOS Release 9.3.

**Description** For aggregated Ethernet interfaces only, configure Link Aggregation Control Protocol (LACP) parameters at the global level for use by LACP at the interface level.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** Configuring Aggregated Devices on page 712.

## lcc

**Syntax**

```
lcc number {
    fpc slot-number {
        pic pic-number {
            atm-cell-relay-accumulation;
            atm-l2circuit-mode (cell | aal5 | trunk trunk);
            framing (sdh | sonet);
            idle-cell-format {
                itu-t;
                payload-pattern payload-pattern-byte;
            }
            max-queues-per-interface (8 | 4);
            no-concatenate;
        }
    }
    online-expected;
    offline;
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure a T640 routing node on a routing matrix.

**Options** *number*—Specifies a T640 routing node on a routing matrix.
**Range:** 0 through 3

The remaining statements are explained separately.

**Usage Guidelines** See "TX Matrix Platform and T640 Routing Node Configuration Guidelines" on page 779 and "Configuring a T640 Routing Node Within a Routing Matrix" on page 782.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** *TX Matrix Platform Hardware Guide*

## link-protection

**Syntax**
```
link-protection {
    non-revertive;
}
```

**Hierarchy Level** [edit chassis aggregated-devices ethernet lacp]

**Release Information** Statement introduced in JUNOS Release 9.3.

**Description** Enable LACP link protection at the global (chassis) level.

**Options** The statements are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** Configuring Aggregated Devices on page 712.

## max-queues-per-interface

**Syntax** max-queues-per-interface (8 | 4);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** On M320, T320, and T640 routing platforms, and TX Matrix platforms, configure eight egress queues on IQ interfaces.

**Usage Guidelines** See "Configuring Eight Queues on IQ Interfaces" on page 760.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## mlfr-uni-nni-bundles

**Syntax** mlfr-uni-nni-bundles *number*;

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure link services management properties.

**Options** *number*—Number of Multilink Frame Relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles to allocate on a Link Services PIC.
**Range:** 1 through 128
**Default:** 16

**Usage Guidelines** See "Configuring the Link Services PICs" on page 767. See also the *JUNOS Network Interfaces Configuration Guide*.

**Required Privilege Level** chassis—To view this statement in the configuration.
chassis-control—To add this statement to the configuration.

## network-services

**Syntax** network-services (ethernet | ip);

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 8.5.

**Description** Use the set network-services statement to set the router's network services to either Ethernet or to Internet Protocol (IP).

**Options** ethernet—Set the router's network services to Ethernet.

ip—Set the router's network services to Internet Protocol.

**Usage Guidelines** See "Configuring the IP and Ethernet Services Mode in MX-series Routers" on page 777.

**Required Privilege Level** chassis—To view this statement in the configuration.
chassis-control—To add this statement to the configuration.

## no-concatenate

**Syntax** no-concatenate;

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number*] (Routing Matrix)

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Do not concatenate (multiplex) the output of a SONET/SDH PIC (an interface with a name so-*fpc/pic/port*).

When configuring and displaying information about interfaces that are operating in channelized mode, you must specify the channel number in the interface name (*physical:channel*); for example, so-2/2/0:0 and so-2/2/0:1. For more information about interface names, see the *JUNOS Network Interfaces Configuration Guide*.

On SONET OC48 interfaces that are configured for channelized (multiplexed) mode, the bytes e1-quiet and bytes f1 options in the sonet-options statement have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0. They work in the transmit direction only on channels 1, 2, and 3.

**Default** Output is concatenated (multiplexed).

**Usage Guidelines** See "Configuring Channelized PIC Operation" on page 757.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** *JUNOS Network Interfaces Configuration Guide* and TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## non-revertive

**Syntax** non-revertive;

**Hierarchy Level** [edit chassis aggregated-devices ethernet lacp link-protection]

**Release Information** Statement introduced in JUNOS Release 9.3.

**Description** Disable the ability to switch to a better priority link (if one is available) once a link is established as active and a collection or distribution is enabled.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Topics** Configuring Aggregated Devices on page 712.

## offline

**Syntax** offline;

**Hierarchy Level** [edit chassis lcc *number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Routing matrix only) Configure a T640 routing node so that it is not part of the routing matrix.

**Usage Guidelines** See "Configuring the Online Expected Alarm" on page 785.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** online-expected and TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## on-disk-failure

**Syntax**
```
on-disk-failure {
    disk-failure-action (halt | reboot);
}
```

**Hierarchy Level** [edit chassis routing-engine]

**Release Information** Statement introduced before JUNOS Release 7.4.
The disk-failure-action statement added in JUNOS Release 9.0.

**Description** Instruct the router to halt or reboot if it detects hard disk errors on the Routing Engine.

**Options** The remaining statement is explained separately.

**Usage Guidelines** See "Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors" on page 772.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## online-expected

**Syntax** online-expected;

**Hierarchy Level** [edit chassis lcc *number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** (Routing matrix only) Configure a T640 routing node so that if it does not come online, an alarm is sent to the TX Matrix platform.

**Usage Guidelines** See"Configuring the Online Expected Alarm" on page 785.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** offline and TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## packet-scheduling

**Syntax** (packet-scheduling | no-packet-scheduling);

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Enable packet-scheduling mode, in which the Packet Director application-specific integrated circuit (ASIC) schedules packet dispatches to compensate for transport delay differences. This preserves the interpacket gaps as the packets are distributed from the Packet Director ASIC to the Packet Forwarding Engine.

**Default** no-packet-scheduling

**NOTE:** The packet-scheduling feature is available on M160 routers only.

**Options** no-packet-scheduling—Do not schedule packets.

packet-scheduling—Schedule packets to preserve interpacket gaps.

**Usage Guidelines** See "Configuring Packet Scheduling" on page 766.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## pem

**Syntax**

```
pem {
    minimum number;
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure the minimum number of PEMs on an M320 router. With this configuration, PEM absent alarms are generated only if the PEM count falls below the minimum specified.

**Options** *number*—Minimum number of PEMs on the router.
**Range:** 0 through 3

**Usage Guidelines** See "Configuring an Entry-Level M320 Router" on page 775.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** sib

## pic

See the following topics:



### *pic (M-series and T-series Routing Platforms)*

**Syntax**

```
pic pic-number {
    ce1 {
        e1 port-number {
            channel-group group-number timeslots slot-number;
        }
    }
    ct3 {
        port port-number {
            t1 link-number {
                channel-group group-number timeslots slot-number;
            }
        }
    }
    framing (sdh | sonet);
    idle-cell format {
        itu-t;
        payload-pattern payload-pattern-byte;
    }
    max-queues-per-interface (8 | 4);
    no-concatenate;
}
```

**Hierarchy Level** [edit chassis fpc *slot-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure properties for an individual PIC.

**Options** *pic-number*—Slot number in which the PIC is installed.
**Range:** 0 through 3

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See "Configuring SONET/SDH Framing" on page 754, "Configuring Channelized PIC Operation" on page 757, "Configuring Channelized DS3-to-DS0 Naming" on page 758, and "Configuring Channelized E1 Naming" on page 761.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

### *pic (TX Matrix Platform)*

**Syntax**
```
pic pic-number {
    atm-cell-relay-accumulation;
    atm-l2circuit-mode (cell | aal5 | trunk trunk);
    framing (sdh | sonet);
    idle-cell-format {
        itu-t;
        payload-pattern payload-pattern-byte;
    }
    max-queues-per-interface (8 | 4);
    no-concatenate;
    q-pic-large-buffer <large-scale | small-scale>;
}
```

**Hierarchy Level** [edit chassis lcc *number* fpc *slot-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** On a TX Matrix platform, configure properties for an individual PIC.

**Options** *pic-number*—Slot number in which the PIC is installed.
**Range:** 0 through 3

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See "Configuring SONET/SDH Framing" on page 754.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 779.

## port

**Syntax**
```
port port-number;
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* ct3]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the channelized T3 port number on the PIC.

**Options** *pic-number*—Port number.
**Range:** 0 through 1

**Usage Guidelines** See "Configuring Channelized DS3-to-DS0 Naming" on page 758.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## power

**Syntax** power (off | on);

**Hierarchy Level** [edit chassis fpc *slot-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure the Flexible PIC Concentrator (FPC) to stay offline or to come online automatically.

**Default** on

**Options** off—Take the FPC offline, and configure it to stay offline, as, for example, after a system reboot.

on—Bring the FPC online, and configure it to come online automatically, as, for example, after a system reboot.

**Usage Guidelines** See "Configuring a Flexible PIC Concentrator to Stay Offline" on page 711.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## q-pic-large-buffer

**Syntax** q-pic-large-buffer <large-scale | small-scale>;

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure delay buffers.

**Default** small-scale

**Options** large-scale—Set the average packet size used to calculate the number of notification queue entries in the IQ PIC to 256 bytes. Useful for slower interfaces (T1, E1, and *N*xDS0 interfaces configured on Channelized IQ PICs and Gigabit Ethernet VLANs configured on Gigabit Ethernet IQ PICs).

small-scale—Set the average packet size used to calculate the number of notification queue entries in the IQ PIC to 40 bytes.

**Usage Guidelines** See "Configuring Larger Delay Buffers" on page 774.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** *JUNOS Class of Service Configuration Guide*

## red-buffer-occupancy

**Syntax**
```
red-buffer-occupancy {
   weighted-averaged <instant-usage-weight-exponent weight-value>;
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number*] (Routing Matrix)

**Release Information** Statement introduced in JUNOS Release 8.3.

**Description** Configure computation of buffer occupancy weighted RED (WRED) based on weighted-averaging of buffer occupancy on an IQ PIC.

**Options** *instant-usage-weight-exponent*—Establish a value to use for weighted average calculations of buffer occupancy.

*weight-value*—Establish an exponent to use for weighted average calculations of buffer occupancy.
**Range:** For IQ PICs, 1 through 31.

Values in excess of 31 are configurable, and appear in show commands, but are replaced with the operational maximum value of 31 on IQ PICs.

**Usage Guidelines** See the *JUNOS Class of Service Configuration Guide*.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## routing-engine

**Syntax**

```
routing-engine {
    on-disk-failure {
        disk-failure-action (halt | reboot);
    }
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 7.4.
The disk-failure-action statement added in JUNOS Release 9.0.

**Description** Configure a Routing Engine to halt or reboot automatically when a hard disk error occurs. A hard disk error may cause a Routing Engine to enter a state in which it responds to local pings and interfaces remain up, but no other processes are responding. Rebooting or halting prevents this.

**Usage Guidelines** See "Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors" on page 772.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** For information about the routing-engine statement at the [edit chassis redundancy] hierarchy level, see the *JUNOS High Availability Configuration Guide*.

## sfm

**Syntax** sfm *slot-number* power off;

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For routers with SFMs, configure an SFM to stay offline.

By default, if you use the request chassis sfm CLI command to take an SFM offline, the SFM will attempt to restart when you enter a commit CLI command. To prevent a restart, configure an SFM to stay offline. This feature is useful for repair situations. The SFM remains offline until you delete this statement.

**Options** *slot-number*—Slot number in which the SFM is installed.

power off—Take the SFM offline and configure it to remain offline.

**Usage Guidelines** See "Configuring an SFM to Stay Offline" on page 711.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** For information about the sfm statement at the [edit chassis redundancy] hierarchy level, see the *JUNOS High Availability Configuration Guide*.

## service-package

**Syntax** service-package (layer-2 | layer-3);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* adaptive-services]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For adaptive services interfaces, enable a service package on the specified Physical Interface Card (PIC).

**Options** layer-2—Enable a Layer 2 service package on the specified PIC.

layer-3—Enable a Layer 3 service package on the specified PIC.

**Usage Guidelines** See "Configuring Service Packages on Adaptive Services Interfaces" on page 753.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** *JUNOS Services Interfaces Configuration Guide* and *JUNOS Feature Guide*.

## sib

**Syntax**
```
sib {
    minimum number;
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in JUNOS Release 7.4.

**Description** Configure the minimum number of SIBs on an M320 router. With this configuration, SIB absent alarms are generated only if the SIB count falls below the minimum specified.

**Options** *number*—Minimum number of SIBs on the router.
**Range:** 0 through 3

**Usage Guidelines** See "Configuring an Entry-Level M320 Router" on page 775.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** pem

## sonet

**Syntax**
```
sonet {
    device-count number;
}
```

**Hierarchy Level** [edit chassis aggregated-devices]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure properties for SONET/SDH aggregated devices on the router.

**Usage Guidelines** See "Configuring Aggregated Devices" on page 712.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## sparse-dlcis

**Syntax** sparse-dlcis;

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*];

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Support a full data-link connection identifier (DLCI) range (1 through 1022). This allows you to use circuit cross-connect (CCC) and translation cross-connect (TCC) features by means of Frame Relay on T1 and E1 interfaces.

**Usage Guidelines** See the "Configuring Sparse DLCI Mode" on page 756.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## synchronization

**Syntax**

```
synchronization {
   signal-type (t1 | e1);
   switching-mode (revertive | non-revertive);
   y-cable-line-termination;
   transmitter-enable;
   validation-interval seconds;
   primary (external-a | external-b);
   secondary (external-a | external-b);
}
```

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in JUNOS Release 7.6.
Statement introduced on the M120 router in JUNOS Release 9.3.

**Description** Juniper Networks M320, M40e, and M120 routing platforms support an external synchronization interface that can be configured to synchronize the internal Stratum 3 clock to an external source, and then synchronize the chassis interface clock to that source.

**Options**

signal-type—Specify the line encoding mode for interfaces: either t1 or e1. For the M40e router, only the t1 signal-type mode is supported.
**Default:** t1

switching-mode—Specify revertive if a lower-priority synchronization can be switched to a valid, higher-priority synchronization.
**Default:** non-revertive

y-cable-line-termination—(M320 routers only) Specify that a single signal be wired to both Control Boards (CBs) using a Y-cable.

transmitter-enable— (M320 routers only) Control whether the diagnostic timing signal is transmitted.

validation-interval—Validate the synchronized deviation. If revertive switching is enabled and a higher-priority clock is validated, the clock module is directed to the higher-priority clock, and all configured and active synchronizations are validated. The validation timer resumes after the current validation interval expires.
**Range:** (M320 and M40e routers) **90** through **86400** seconds (M120 routers) 30 through 86400 seconds
**Default:** (M320 and M40e routers): 90 seconds (M120 routers):30 seconds

primary—First external timing source specified in the configuration hierarchy.

secondary—Second external timing source specified in the configuration hierarchy.

**Usage Guidelines** See “Configuring an External Synchronization Interface” on page 755.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## system-priority

**Syntax** system-priority *priority*;

**Hierarchy Level** [edit chassis aggregated-devices ethernet lacp]

**Release Information** Statement introduced in JUNOS Release 9.3.

**Description** Define LACP system priority for aggregated Ethernet interfaces at the global (chassis) level.

**Options** *priority*—Priority for the aggregated Ethernet system. A smaller value indicates a higher priority.
**Range:** 0 through 65535
**Default:** 127

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** Configuring Aggregated Devices on page 712

## t1

**Syntax**
```
t1 link-number {
    channel-group group-number timeslots slot-number;
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* ct3 port *port-number*];

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure channelized T1 port and channel specifications.

**Options** *link-number*—T1 link.
**Range:** 0 through 27 for DS0 naming

The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Configuring Channelized DS3-to-DS0 Naming” on page 758.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## timeslots

**Syntax** timeslots *slot-number*;

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* ct3 port *port-number* t1 *link-number* channel-group *channel-number*],
[edit chassis fpc *slot-number* pic *pic-number* ce1 e1*link-number* channel-group *channel-number*]
[edit chassis lcc *lcc-index* fpc *slot-number* pic *pic-number* ct3 port *port-number* t1 *link-number* channel-group *channel-number*],
[edit chassis lcc *lcc-index* fpc *slot-number* pic *pic-number* ce1 e1*link-number* channel-group *channel-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** For E1 or T1 interfaces, allocate the specific time slots by number.

**Options** *slot-number*—Actual time slot number(s) allocated.
**Range:** 1 through 24 for T1 and 1 through 32 for E1
**Default:** All time slots for T1 and all time slots for E1

**Usage Guidelines** See "Configuring Channelized DS3-to-DS0 Naming" on page 758 and "Configuring Channelized E1 Naming" on page 761.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## traffic-manager

**Syntax**
```
traffic-manager {
    ingress-shaping-overhead number;
    mode session-shaping;
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number*] (Routing Matrix)

**Release Information** Statement introduced in JUNOS Release 8.3.

**Description** Enable shaping on an L2TP session.

The remaining statements are explained separately.

**Usage Guidelines** See the *JUNOS Class of Service Configuration Guide*.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## tunnel-services

**Syntax** tunnel-services {
bandwidth (1g | 10g);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *number*]

**Release Information** Statement introduced in JUNOS Release 8.2.

**Description** For MX-series Ethernet Services Routers, configure the amount of bandwidth for tunnel services.

**Options** The statements are explained separately.

**Usage Guidelines** See "Configuring Tunnel Interfaces on MX-Series Ethernet Services Routers" on page 764.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

## vrf-mtu-check

**Syntax** vrf-mtu-check;

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** On M-series routers (except the M320 router), configure path maximum transmission unit (MTU) checks on the outgoing interface for unicast traffic routed on a virtual private network (VPN) routing and forwarding (VRF) instance.

**Default** Disabled.

**Usage Guidelines** See "Configuring an MTU Path Check for a Routing Instance" on page 768.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Topics** *JUNOS Network Interfaces Configuration Guide*

## vtmapping

**Syntax** vtmapping (klm | itu-t);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number*]

**Release Information** Statement introduced before JUNOS Release 7.4.

**Description** Configure virtual tributary mapping.

**Default** klm

**Options** klm—KLM standard.

itu-t—International Telephony Union standard.

**Usage Guidelines** See "Configuring Channelized STM1 Interface Virtual Tributary Mapping" on page 762.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

# Part 7
# Index

# Index

## B

## C

## D

## E



## F

## G



## H



## I

## J



## K



## L

## M

## N



## O

## P

## Q



## R

## S

## T

## U



## V



## W



## X



## Y

# Index of Statements and Commands

## D



## E



## F



## G



## H



## I

## K



## L



## M



## N



## O



## P

## Q



## R



## S

## T



## U



## V



## W



## X