Junos® OS

System Basics Configuration Guide

Release
11.2

Published: 2011-05-17

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

Junos® OS System Basics Configuration Guide
Release 11.2

Revision History
April 2011—R1 Junos OS 11.2

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 OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

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 Index

List of Figures

List of Tables

About This Guide

This preface provides the following guidelines for using the *Junos® OS System Basics Configuration Guide*:

Junos OS Documentation and Release Notes

For a list of related Junos OS documentation, see http://www.juniper.net/techpubs/software/junos/ .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS Release Notes.*

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

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books .

Objectives

This guide describes Juniper Networks routers 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.

NOTE: For additional information about the Junos OS—either corrections to or information that might have been omitted from this guide—see the software release notes at http://www.juniper.net/ .

Audience

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.

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 OS 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 OS CLI User Guide*.

Documentation Conventions

Table 1 on page xliv 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 xlv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name *domain-name***
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	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** (***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]
		routing-options {
		  static {
		    route default {
		      nexthop *address*;
		      retain;
		    }
		  }
		}

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

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

Convention	Description	Examples
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**. • 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**.

Documentation Feedback

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

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

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Introduction to Junos OS

Junos OS Overview

Juniper Networks provides high-performance network routers that create a responsive and trusted environment for accelerating the deployment of services and applications over a single network. Junos OS is the foundation of these high-performance networks. Unlike other complex, monolithic software architectures, Junos OS incorporates key design and developmental differences to deliver increased network availability, operational efficiency, and flexibility. These key advantages 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, Junos OS is a single, cohesive operating system that is shared across all routers and product lines. This enables Juniper Networks engineers to develop software features once and share the features across all 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. Furthermore, because all Juniper

Networks products use the same code base, interoperability among products is not an issue.

One Software Release

Each new version of Junos OS is released concurrently for all product lines following a preset quarterly schedule. Each new version of 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 OS communicate through well-defined interfaces, each module runs in its own protected memory space, preventing one module from disrupting another. It also enables 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 Junos OS is preinstalled on your Juniper Networks router when you receive it from the factory. Thus, when you first power on the router, all software starts automatically. You simply need to configure the software so that the router can participate in the network.

You can upgrade the router software as new features are added or software problems are fixed. You normally obtain new software by downloading the images from the Juniper Networks Support Web page onto your router or onto another system on your local network. Then you install the software upgrade onto the router.

Juniper Networks routers run only binaries supplied by Juniper Networks. Each Junos OS image includes a digitally signed manifest of executables, which are registered with the system only if the signature can be validated. Junos OS will not execute any binary without a registered fingerprint. This feature protects the system against unauthorized software and activity that might compromise the integrity of your router.

Related Documentation

- Junos OS Architecture Overview on page 5
- Router Hardware Components on page 7
- Junos OS Commit Model for Router or Switch Configuration on page 8
- Junos OS Routing Engine Components and Processes on page 9
- Junos OS Support for IPv4 Routing Protocols on page 11
- Junos OS Support for IPv6 Routing Protocols on page 13
- Junos OS Routing and Forwarding Tables on page 14
- Routing Policy Overview on page 14
- Junos OS Support for VPNs on page 15

Junos OS Architecture Overview

This topic provides an overview of the Junos OS product and routing process architecture:

- Product Architecture on page 5
- Routing Process Architecture on page 5

Product Architecture

The Junos OS provides IP routing protocol software as well as software for interface, network, and chassis management. The Junos OS runs on all Juniper Networks J Series, M Series, MX Series, and T Series routers.

- 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 3D Universal Edge 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 routers (T320, T640, T1600, TX Matrix, and TX Matrix Plus routers) are deployed at the core of provider networks. These routers have fully redundant hardware, including power and cooling, Routing Engines, and Switch Interface Boards.

  A *routing matrix* is a multichassis architecture composed of either one TX Matrix router and from one to four T640 routers connected to the TX Matrix router, or one TX Matrix Plus router and from one to four T1600 routers connected to the TX Matrix Plus router. From the perspective of the user interface, the routing matrix appears as a single router. On a routing matrix composed of a TX Matrix router and T640 routers, the TX Matrix router controls all the T640 routers. On a routing matrix composed of a TX Matrix Plus router and T1600 routers, the TX Matrix Plus router controls all the T1600 routers.

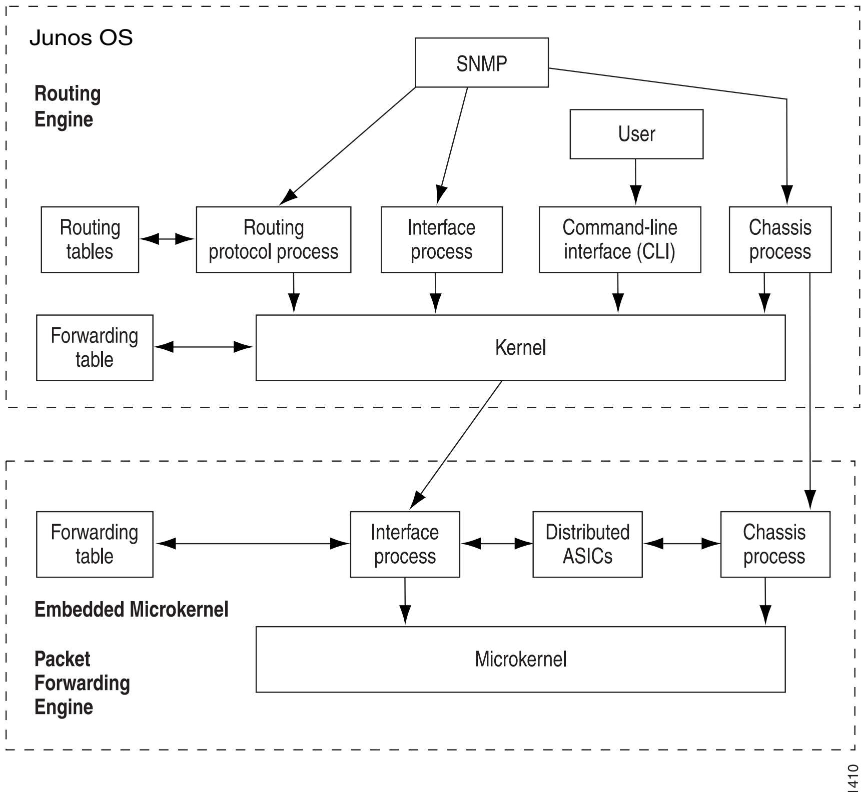
Routing Process Architecture

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

- Routing Engine
- 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.

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 routers' interfaces, some of the chassis components, system management, and user access to the router. These routers and software processes run on top of a kernel that interacts with the Packet Forwarding Engine. All M Series (except the M7i and M40) routers and T Series routers have redundant Routing Engines.

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 OS 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 router'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.

Related Documentation

- Junos OS Overview on page 3

Router Hardware Components

The Junos OS runs on four types of Juniper Networks routers: J Series, M Series, MX Series, and T Series. The routers consist of the major hardware components as shown in Table 3 on page 7. One or more of the major hardware components shown is used in each system.

Table 3: Major Router Hardware Components

	M Series	MX Series	T Series	J Series
Routing Engines (RE)	X	X	X	X

Table 3: Major Router Hardware Components *(continued)*

	M Series	MX Series	T Series	J Series
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 routers, the PICs are installed directly in the chassis.

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

Related Documentation

- Junos OS Architecture Overview on page 5

Junos OS Commit Model for Router or Switch Configuration

The router or switch configuration is saved using a commit model: that is, a candidate configuration is modified as desired and then committed to the system. Once a configuration has been committed, the router or switch 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 or switch can have a maximum of 49 rollback configurations (1–49) saved on the system.

On the router or switch, 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 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 router or switch:

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

  NOTE: The QFX3500 switch has only one routing engine.

  To synchronize 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 router or switch. 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 or switch remote from the router or switch where the command was issued, the synchronization fails on the remote router or switch. You need to clear the lock and reissue the synchronization command.

Related Documentation

- Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine on page 23

Junos OS Routing Engine Components and Processes

The Junos OS runs on the Routing Engine. The Junos OS consists of software processes that support Internet routing protocols, control router interfaces and the router chassis, and enable router system management. The Junos OS 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 OS can be used to configure routing protocols and router interface properties, as well as to monitor and troubleshoot protocol and network connectivity problems.

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

Routing Engine Kernel

The Routing Engine kernel provides the underlying infrastructure for all Junos OS 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 OS, 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 Junos XML protocol XML requests from its client, which may be the command-line interface (CLI) or any Junos XML protocol client.

Process Limits

There are limits to the total number of Junos OS 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.

There are limits to the total number of Junos OS 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 OS, 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 enables 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.

Interface Process

The Junos interface process enables 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 OS to track the status and condition of the router's interfaces.

Chassis Process

The Junos chassis process enables 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 OS 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.

Related Documentation

- Junos OS Architecture Overview on page 5

Junos OS Support for IPv4 Routing Protocols

Junos OS 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 OS 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 enables 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 enables 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 enables 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, enables 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.

Related Documentation

- Junos OS Overview on page 3
- Junos OS Support for IPv6 Routing Protocols on page 13

Junos OS Support for IPv6 Routing Protocols

The Junos OS 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 enables 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 OS 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.

Related Documentation

- Junos OS Overview on page 3
- Junos OS Support for IPv4 Routing Protocols on page 11

Junos OS 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.

Related Documentation

- Routing Policy Overview on page 14

Routing Policy Overview

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 enables 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 enables you to set the information associated with a route as it is being imported into or exported from the routing table. Filtering imported routes enables you to control the routes used to determine active routes. Filtering routes being exported from the routing table enables 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.

Related Documentation

- Junos OS Routing and Forwarding Tables on page 14
- Junos OS Support for IPv4 Routing Protocols on page 11
- Junos OS Support for IPv6 Routing Protocols on page 13

Junos OS Support for VPNs

The Junos OS 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.

Related Documentation

- Junos OS Overview on page 3

CHAPTER 2

Junos Configuration Basics

This chapter includes the following topics:

Junos OS Configuration Basics

Your router comes with Junos OS 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 OS, you must specify a hierarchy of configuration statements that define the preferred software properties. You can configure all properties of the Junos OS, 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 OS.

Related Documentation

- Junos OS Configuration from External Devices on page 17
- Methods for Configuring Junos OS on page 19
- Initial Router or Switch Configuration Using the Junos OS on page 22

Junos OS Configuration from External Devices

You can configure the router from a system console connected to the router'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 OS:

- 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.

Related Documentation

- Methods for Configuring Junos OS on page 19
- Configuring the Junos OS to Set Console and Auxiliary Port Properties on page 234

Methods for Configuring Junos OS

You can use any of the methods shown in Table 4 on page 19 to configure Junos OS:

Table 4: Methods for Configuring Junos OS

Method	Description
Command-line interface (CLI)	Create the configuration for the device 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 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 thedevice. 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. J-Web is not available for the QFX Series.
Junos XML management protocol (API)	Use Junos XML protocol Perl client modules to develop custom applications for configuring information on devices that run Junos OS. Client applications use the Junos XML management protocol to request and change configuration information on Juniper Networks J Series, M Series, and T Series routers. The Junos XML management protocol is customized for Junos OS, and operations in the API are equivalent to those in the Junos OS CLI.
NETCONF application programming interface (API)	Use NETCONF Perl client modules to develop custom applications for configuring information on devices that run Junos OS. Client applications use the NETCONF XML management protocol to request and change configuration information on Juniper Networks J Series, M Series, and T Series routers. The NETCONF XML management protocol 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). Commit scripts are not available for the QFX Series.

The following sections contain complete descriptions of the methods you can use to configure Junos OS:

- Junos OS Command-Line Interface (CLI) on page 20
- ASCII File on page 20
- J-Web Package on page 20
- Junos XML Management Protocol Software on page 21

- NETCONF XML Management Protocol Software on page 21
- Configuration Commit Scripts on page 21

Junos OS Command-Line Interface (CLI)

The Junos OS 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 OS CLI User Guide* and *Junos OS System Basics and Services Command Reference*.

ASCII File

You can load an ASCII file containing a 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 OS supports the 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 routers. 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 routers, follow the procedure described in the *Junos OS 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 OS 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 OS System Basics and Services Command Reference*.

Junos XML Management Protocol Software

The Junos XML management protocol 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 routers. This API is customized for Junos OS, and operations in the API are equivalent to Junos OS CLI configuration mode commands. The Junos XML management protocol includes a set of Perl modules that enable client applications to communicate with a Junos XML protocol server on the router. The Perl modules are used to develop custom applications for configuring and monitoring Junos OS.

For a complete description of how to use Junos XML and Junos XML management protocol software, see the *Junos XML Management Protocol Guide*.

NETCONF XML Management Protocol Software

The NETCONF XML management protocol 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 routers. This API is customized for Junos OS, and includes features that accommodate the configuration data models of multiple vendors. The NETCONF XML management protocol 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 OS.

For a complete description of how to use Junos XML and NETCONF XML management protocol software, see the *NETCONF XML Management Protocol 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 OS 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 OS Configuration and Operations Automation Guide*.

Related Documentation

- Junos OS Configuration from External Devices on page 17

Configuring a Router for the First Time

This section includes the following topics:

Initial Router or Switch Configuration Using the Junos OS

This topic provides an overview of initial router or switch configuration tasks using the Junos OS.

When you turn on a router or switch for the first time, the Junos OS automatically boots and starts. You must enter basic configuration information so that the router or switch is on the network and you can log in to it over the network.

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

When you first connect to the router or switch 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 command prompt shows the username **root@#**.

You must start the Junos OS 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 OS operational mode. Enter the Junos OS configuration mode by typing the command **configure**. The command prompt **root@#** indicates that you are in the Junos OS configuration mode.

When you first configure a router or switch, you must configure the following basic properties:

- Router or switch hostname
- Domain name
- IP address of the router or switch Ethernet management interface—On all routers other than the TX Matrix Plus router and the T1600 routers in a routing matrix, the management Ethernet Interface is **fxp0**. On a TX Matrix Plus router and the T1600 routers in a routing matrix, the management Ethernet interface is **em0**.

NOTE: The management Ethernet interface created on a T1600 standalone router (not part of a routing matrix and not connected to a TX Matrix Plus router) continues to be **fxp0** and not **em0**. The **em0** management Ethernet interface is only applicable for a TX Matrix Plus router and T1600 routers connected to a TX Matrix Plus router in a routing matrix.

- IP address of a backup router
- IP address of one or more DNS name servers on your network
- Password for the root account

Related Documentation

- Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine on page 23
- Configuring the Junos OS the First Time on a Router with Dual Routing Engines on page 27
- Junos OS Configuration Using the CLI on page 33

Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine

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

To configure the router initially, you must connect a terminal or laptop computer to the router through the console port—a serial port on the front of the router. 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, are disabled by default.

To configure the Junos OS for the first time on a router with a single Routing Engine, follow these steps:

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

   The Junos OS 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 router shows the username **root@#**.
4. Start the Junos OS command-line interface (CLI):

   ```
   root@# cli
   root@>
   ```
5. Enter Junos OS configuration mode:


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

6. Configure the name of the router (the router hostname). We do not recommend spaces in the router 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 router'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. The management Ethernet interface provides a separate out-of-band management network for the router.

   - For all routers *except* the TX Matrix Plus router and T1600 routers in a routing matrix:

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

   - For a TX Matrix Plus router and T1600 routers in a routing matrix only:

     ```
     [edit]
     root@# set interfaces em0 unit 0 family inet address address/prefix-length
     ```

     To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

   - For a T1600 standalone router (not connected to a TX Matrix Plus router and not in a routing matrix):

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

9. Configure the IP address of a backup or default router. 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 router by way of the management interface. The router 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 routers with two Routing Engines, the backup Routing Engine, **RE1**, uses the backup router as a default gateway after the router boots. This enables you to access the backup Routing Engine. (**RE0** is the default master Routing Engine.)

   NOTE: The backup router Routing Engine does not support more than 16 destinations. If you configure more than 16 destinations on the backup Routing Engine, the Junos OS ignores any destination addresses after the sixteenth address and displays a commit-time warning message to this effect.

   ```
   [edit]
   ```

root@# **set system backup-router** *address*

10. Configure the IP address of a DNS server. The router 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.

    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 ;
        }
      }
    }
  }
}
```

On a TX Matrix Plus router, the management Ethernet interface is **em0** and not **fxp0**. Therefore, when you issue the **show** command in the configuration mode, the configuration statements would be:

```
[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 {
      em0 {
         unit 0 {
            family inet {
               address address ;
            }
         }
      }
   }
}
```

13. Commit the configuration, which activates the configuration on the router:

```
[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 OS defaults are now set on the router.

If you want to configure additional Junos OS properties at this time, remain in the CLI configuration mode and add the necessary configuration statements. You need to commit your configuration changes to activate them on the router.

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 router, 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 router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router'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.

Related Documentation

- Initial Router or Switch Configuration Using the Junos OS on page 22
- Format for Specifying IP Addresses, Network Masks, and Prefixes in Junos OS Configuration Statements on page 45
- Default Directories for Junos OS File Storage on the Router or Switch on page 47
- Configuring Basic Router or Switch Properties on page 62
- Configuring Automatic Mirroring of the CompactFlash Card on the Hard Disk Drive on page 68

Configuring the Junos OS the First Time on a Router with Dual Routing Engines

If a router has dual Routing Engines, you can create configuration groups and use the same configuration for both Routing Engines. This ensures that the configuration will not change during a failover scenario because of the identical configuration shared between the Routing Engines.

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 Routing Engine-specific parameters. 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 router may not forward traffic correctly, because the backup Routing Engine may have a different configuration.

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

1. Go to "Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine" on page 23 and follow Step 1 through Step 5 to initially configure the backup Routing Engine.

2. Create the configuration group **re0**. The **re0** group is a special group designator that is only used by **RE0** in a redundant routing platform.

   [edit]root# **set groups re0**

3. Navigate to the **groups re0** level of the configuration hierarchy.

   [edit]root# **edit groups re0**

4. Specify the router hostname.

   [edit groups re0]root# **set system host-name** ***host-name***

   NOTE: The hostname specified in the router configuration is not used by the DNS server to resolve to the correct IP address. This hostname is used to display the name of the Routing Engine in the CLI. For example, the hostname appears at the command-line prompt when the user is logged in to the CLI:

   user-name@host-name>

5. Configure the IP address and prefix length for the router Ethernet interface.

   - For all routers except the TX Matrix Plus router and T1600 routers in a routing matrix:

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

   - For TX Matrix Plus and T1600 routers in a routing matrix only:

     [edit]
     root@# **edit groups**
     [edit groups]
     root@# **set interfaces em0 unit 0 family inet address** ***address/prefix-length***

     To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

   - For a T1600 standalone router (not connected to a TX Matrix Plus router and not in a routing matrix):

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

6. Set the loopback interface address for **re0** configuration group:

   [edit groups]
   root@# **set re0 interfaces lo0 unit 0 family inet address** ***address/prefix-length***

7. Return to the top level of the hierarchy.

   [edit groups re0]root# **top**

8. Create the configuration group **re1**.

[edit]root# **set groups re1**

9. Navigate to the **groups re1** level of the configuration hierarchy.

   [edit]root# **edit groups re1**

10. Specify the router hostname.

    [edit groups re1]root# **set system host-name** ***host-name***

11. Configure the IP address and prefix length for the router Ethernet interface.

    - For all routers except the TX Matrix Plus router and T1600 routers in a routing matrix:

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

    - For TX Matrix Plus and T1600 routers in a routing matrix only:

      [edit]
      root@# **edit groups**
      [edit groups]
      root@# **set interfaces em0 unit 0 family inet address** ***address/prefix-length***

      To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

    - For a T1600 standalone router (not connected to a TX Matrix Plus router and not in a routing matrix):

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

12. Set the loopback interface address for **re1** configuration group:

    [edit groups]
    root@# **set re1 interfaces lo0 unit 0 family inet address** ***address/prefix-length***

13. Return to the top level of the hierarchy.

    [edit groups re0]root# **top**

14. Configure the **apply-groups** statement to reproduce the configuration group information to the main part of the configuration and to specify the group application order.

    [edit]
    root# **set apply-groups [re0 re1]**

15. 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**

16. Save the configuration change on both Routing Engines:

    [edit]
    user@host> **commit synchronize**

root@#

After the configuration changes are saved, complete the management console configuration.

1. Configure the IP address of the DNS server.

   [edit]root# **set system name-server** ***address***

2. Configure the router domain name:

   [edit]root# **set system domain-name** ***domain-name***

3. Configure the IP address of a backup or default router. 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 router by way of the management interface. The router 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 routers with two Routing Engines, the backup Routing Engine, **RE1**, uses the backup router as a default gateway after the router boots. This enables you to access the backup Routing Engine. (**RE0** is the default master Routing Engine.)

   NOTE: The backup router Routing Engine does not support more than 16 destinations. If you configure more than 16 destinations on the backup Routing Engine, the Junos OS ignores any destination addresses after the sixteenth address and displays a commit-time warning message to this effect.

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

4. 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.

   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***

5. 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 ;
            }
         }
      }
   }
}
```

On a TX Matrix Plus router, the management Ethernet interface is **em0** and not **fxp0**. Therefore, when you issue the **show** command in the configuration mode, the configuration statements would be:

```
[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 {
      em0 {
         unit 0 {
            family inet {
               address address ;
            }
         }
      }
   }
}
```

6. 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 router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router'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.

For more information about creating configuration groups, see *Junos OS CLI User Guide*.

For more information about the iniasequeirtial configuration for redundant Routing Engine systems and the re0 group, see *Junos OS High Availability Configuration Guide*.

Related Documentation

- Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine on page 23
- Initial Router or Switch Configuration Using the Junos OS on page 22
- Format for Specifying IP Addresses, Network Masks, and Prefixes in Junos OS Configuration Statements on page 45
- Default Directories for Junos OS File Storage on the Router or Switch on page 47
- Configuring Basic Router or Switch Properties on page 62
- Configuring Automatic Mirroring of the CompactFlash Card on the Hard Disk Drive on page 68

Junos OS Default Settings for Router Security

The Junos OS protects against common router security weaknesses with the following default settings:

- The Junos OS 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 OS 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 OS 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.

Related Documentation

- Example: Consolidated Security Configuration on page 281

Junos OS Configuration Using the CLI

You configure the Junos OS using the Junos OS command-line interface (CLI). The CLI is described in detail in the *Junos OS 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 consistent syntax. For example, you configure routing protocols, routing policies, interfaces, and SNMP management in their own separate portions of the configuration hierarchy.

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.

Related Documentation

- Disk Space Management for Junos OS Installation on page 34
- Activation of the Junos OS Candidate Configuration on page 33

Activation of the Junos OS Candidate Configuration

You enter software configuration statements using the CLI to create a candidate configuration that contains a hierarchy of statements. 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.

Related Documentation

- Junos OS Commit Model for Router or Switch Configuration on page 8

Disk Space Management for Junos OS Installation

A Junos OS 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 OS:
  - On the J Series routers, 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 routers, 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.

Related Documentation

- Junos OS Configuration Using the CLI on page 33

Junos OS Tools for Monitoring the Router

The primary method of monitoring and troubleshooting the Junos OS, 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.

The Junos OS includes SNMP software, which enables 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.

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.

Related Documentation

- Methods for Configuring Junos OS on page 19
- Junos OS Features for Router Security on page 35

Junos OS Features for 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 OS is extremely stable and robust. The Junos OS also provides features to protect against attacks, allowing you to configure the router to minimize vulnerabilities.

The following are Junos OS features available to improve router security:

Methods of Remote Access for Router Management

When you first install the Junos OS, 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—enables connection to the router through an interface dedicated to router management. Juniper Networks routers support out-of-band management with a dedicated management Ethernet interface, as well as EIA-232 console and auxiliary ports. On all routers other than the TX Matrix Plus router and T1600 routers connected to a TX Matrix Plus router in a routing matrix, the management Ethernet Interface is labeled, **fxp0**. On a TX Matrix Plus router and T1600 routers in a routing matrix, the management Ethernet Interface is labeled **em0**. 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—enables 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.

Junos OS Supported Protocols and Methods for 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 OS 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.

The Junos OS 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 OS also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs).
- MD5 authentication of MSDP peering sessions. This authentication provides protection against spoofed packets being introduced into a peering session.

- 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.

Junos OS Plain-Text Password Requirements

The Junos OS has special requirements when you create plain-text passwords on a router. 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]**

Junos OS Support for Routing Protocol Security Features and IPsec

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 OS 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 OS also supports IKE, which defines mechanisms for key generation and exchange, and manages SAs.

Junos OS Support for 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.

Junos OS Auditing Support for Security

The Junos OS 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 OS 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.

Related Documentation

- Example: Configuring Firewall Filters on page 277
- IPsec Overview on page 585
- Junos OS System Log Configuration Overview on page 139

Upgrading to 64-bit Junos OS

Just like any other operating system, the 64-bit version of the Junos OS can address more memory than the 32-bit version of the operating system. In order to support larger Routing Engine memory sizes, an upgrade from the 32-bit to the 64-bit Junos OS running on the Routing Engine hardware is necessary. The upgrade path is relatively straightforward and another form of Routing Engine hardware and software upgrade. However, there are three different and distinct Routing Engine configurations that must be taken into account when upgrading to the 64-bit Junos OS. This topic covers all three.

NOTE:
The 64-bit Junos OS is supported on the following Routing Engines only:

- RE-DUO-C2600-16G
- RE-A-1800x2-16G
- RE-S-1800x4-16G
- RE-JCS1200-1x2330

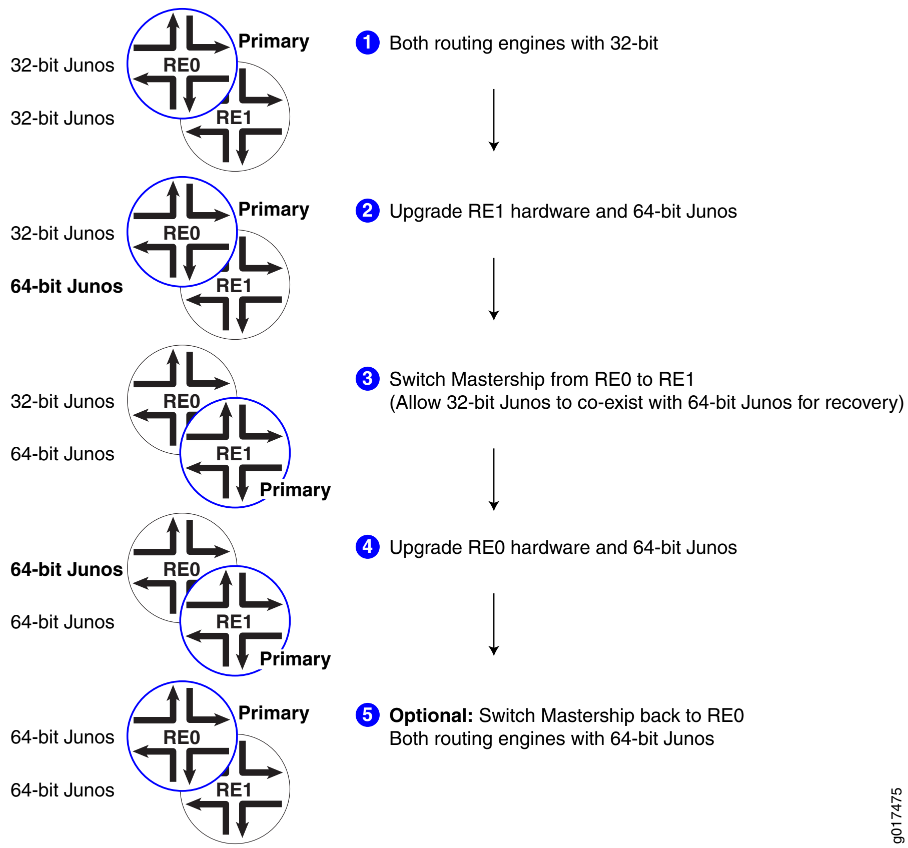
Before you begin, you must have:

- A properly configured and functional router
- One or two Routing Engines installed that support the 64-bit Junos OS
- Decided to allow single Routing Engines systems to use either slot 0 or slot 1 as master or not (this decision will determine which upgrade path to follow for single Routing Engine systems)

When you upgrade a Routing Engine to the 64-bit Junos OS, you can support larger Routing Engine memory sizes. However, the exact procedure depends on whether there are one or two Routing Engines installed. For systems with a single Routing Engine, the procedure varies based on whether the master Routing Engine must always be in slot 0 or not.

To upgrade a system with two Routing Engines, refer to Figure 2 on page 40 and perform the following steps:

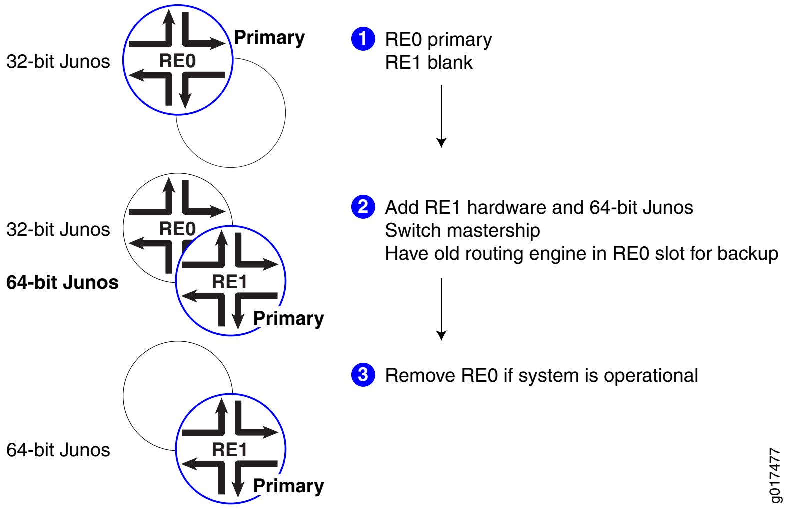
Figure 2: Upgrading to the 64-bit Junos OS with Dual Routing Engines



1. In the initial state, both Routing Engines are running the 32-bit Junos OS, and slot 0 has the master Routing Engine.
2. Upgrade the slot 1 Routing Engine hardware and install the 64-bit Junos OS.
3. Switch the master Routing Engine from slot 0 to slot 1 (allow the 32-bit Junos OS to co-exist with the 64-bit Junos OS).
4. Upgrade the slot 0 routing engine hardware and install the 64-bit Junos OS.
5. Both Routing Engines now run the 64-bit Junos OS. Optionally, you can switch the master Routing Engine back to slot 0.

To upgrade a system with a single Routing Engine, where the master Routing Engine can be in either slot 0 or slot 1, refer to Figure 2 on page 40and perform the following steps:

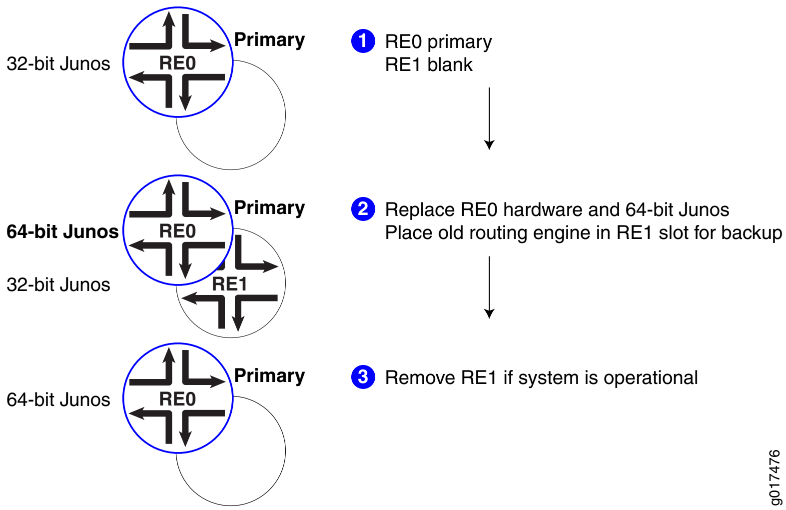
Figure 3: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master in Either Slot)



1. In the initial state, the slot 0 Routing Engine is running the 32-bit Junos OS and slot 1 is blank.
2. Install the upgraded Routing Engine hardware in slot 1 and install the 64-bit Junos OS.
3. When the 64-bit Junos OS is configured properly, remove the slot 0 Routing Engine running the 32-bit Junos OS.

To upgrade a system with a single Routing Engine, where the master Routing Engine must in slot 0, refer to Figure 4 on page 42 and perform the following steps:

Figure 4: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master Must Be in Slot 0)



1. In the initial state, the slot 0 Routing Engine is running the 32-bit Junos OS and slot 1 is blank.
2. Install the slot 0 Routing Engine hardware in slot 1. Install the upgraded Routing Engine hardware in slot 0 and install the 64-bit Junos OS.
3. When the 64-bit Junos OS is configured properly, remove the slot 1 routing engine running the 32-bit Junos OS.

Related Documentation

- Checklist for Reinstalling Junos OS

PART 2

System Management

This chapter includes the following topics:

CHAPTER 3

System Management Overview

The Junos OS 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 provides you an overview of system management functions and features:

Format for Specifying IP Addresses, Network Masks, and Prefixes in Junos OS Configuration Statements

Many statements in the Junos OS configuration include an option to specify an IP address or route prefix. 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 from 1 through 32.

Related Documentation

- Format for Specifying Filenames and URLs in Junos OS CLI Commands on page 46

Format for Specifying Filenames and URLs in Junos OS CLI Commands

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 either one TX Matrix router and from one to four T640 routers connected to the TX Matrix router, or one TX Matrix Plus router and from one to four T1600 routers connected to the TX Matrix Plus router. From the perspective of the user interface, the routing matrix appears as a single router. On a routing matrix composed of the TX Matrix router and T640 routers, the TX Matrix router controls all the T640 routers. On a routing matrix composed of a TX Matrix Plus router and T1600 routers, the TX Matrix Plus router controls all the T1600 routers.

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 (not applicable on the QFX Series). 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 router or a T1600 router in a routing matrix:

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

- **a:*filename*** or **a:*path/filename***—File on the local removable media. 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 OS. 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/%2Fpath/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 router or a T1600 router in a routing matrix:

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

  A *routing matrix* is a multichassis architecture composed of either one TX Matrix router and from one to four T640 routers connected to the TX Matrix router, or one TX Matrix Plus router and from one to four T1600 routers. From the perspective of the user interface, the routing matrix appears as a single router. On a routing matrix composed of the TX Matrix router and T640 routers, the TX Matrix router controls all the T640 routers. On a routing matrix composed of a TX Matrix Plus router and T1600 routers, the TX Matrix Plus router controls all the T1600 routers.

Related Documentation

- Format for Specifying IP Addresses, Network Masks, and Prefixes in Junos OS Configuration Statements on page 45
- Default Directories for Junos OS File Storage on the Router or Switch on page 47

Default Directories for Junos OS File Storage on the Router or Switch

Junos OS files are stored in the following directories on the router or switch:

- **/altconfig**—When you back up the currently running and active file system partitions on the router or switch 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 device from which the router or switch booted (generally the CompactFlash card (device **wd0**) or internal flash storage . This directory contains the current operational router or switch

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 located either on the hard disk (device **wd2**) or internal flash storage. 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 the user's home directory unless the user specifies a full pathname.
  - **/var/db/config**—Contains 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 or switch ships with removable media (device **wfd0**) that contains a backup copy of the Junos OS.

Directories on the Logical System

Logical systems have their individual directory structure created in the **/var/logical-system/*logical-system-name*** directory. It contains the following subdirectories:

- **/config**—Contains the current operational configuration specific to the logical system.
- **/log**—Contains system log and tracing files specific to the logical system.

  To maintain backward compatibility for the log files with previous versions of Junos OS, a symbolic link (symlink) from the **/var/logs/*logical-system-name*** directory to the **/var/logical-systems/*logical-system-name*** directory is created when a logical system is configured.
- **/tmp**—Contains temporary files specific to the logical system.

The new file system for each logical system enables logical system users to view trace logs and modify logical system files. Logical system administrators have full access to view and modify all files specific to the logical system.

Logical system users and administrators can now save and load configuration files at the logical-system level using the **save** and **load** configuration mode commands. In addition, they can also issue the **show log**, **monitor**, and **file** operational mode commands at the logical-system level.

Related Documentation

- Format for Specifying Filenames and URLs in Junos OS CLI Commands on page 46

Junos OS 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 OS 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 at the **[edit system]** hierarchy level. 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 level. This feature does not alter local tracing functionality in any way, and logging files are stored on the router.

The Junos OS 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 "Junos OS System Log Configuration Overview" on page 139, and by using the **options** statement at the **[edit routing-options]** hierarchy level, as described in the *Junos OS 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.
- 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 OS 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 file(s) 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.

  NOTE: When remote tracing is configured, traces will go to the remote host.

  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.

Related Documentation

- Junos OS System Log Configuration Overview on page 139

Junos OS Authentication Methods for Routing Protocols

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.

Related Documentation

- Example: Configuring the BGP and IS-IS Routing Protocols on page 274
- Special Requirements for Junos OS Plain-Text Passwords on page 72

Junos OS User Authentication Methods

The Junos OS 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 OS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

Related Documentation

- Configuring RADIUS Authentication on page 103
- Configuring TACACS+ Authentication on page 108
- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 116

- Configuring RADIUS Authentication
- Configuring TACACS+ Authentication

CHAPTER 4

System Management Configuration Statements

This chapter includes the following topics:

System Management Configuration Statements

This topic lists all the configuration statements that you can include at the **[edit system]** hierarchy level to configure system management features:

```
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;
    }
}
allow-v4mapped-packets;
arp {
    aging-timer minutes;
    gratuitous-arp-delay;
    gratuitous-arp-on-ifup;
    interfaces;
    passive-learning;
    purging;
}
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;
    (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 {
        access-end;
        access-start;
        allow-commands "regular-expression";
        allow-configuration-regexps "regular expression 1" "regular expression 2";
        allowed-days;
        deny-commands "regular-expression";
        deny-configuration-regexps "regular expression 1" "regular expression 2";
        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 {
            (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 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 {
    accounting-port port-number;
    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 {
            optional;
            refresh;
            refresh-from url;
            source url;
        }
        traceoptions {
            file <filename> <files number> <size size> <world-readable | no-world-readable>;
            flag flag;
            no-remote-trace;
    }
```



```
    op {
      file filename {
        arguments {
          argument-name {
            description descriptive-text;
          }
        }
        command filename-alias;
        description descriptive-text;
        refresh;
        refresh-from url;
        source url;
      }
      refresh;
      refresh-from url;
      traceoptions {
        file <filename> <files number> <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
      }
    }
  }
  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;
        }
        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;
        archive <archive-sites {ftp-url <password password>}> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
            no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data;
    }
    host (hostname | other-routing-engine | scc-master) {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string;
        match "regular-expression";
        source-address source-address;
    }
    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 (GMThour-offset | time-zone);
  }
  tracing {
    destination-override {
    syslog host;
    }
  }
  use-imported-time-zones;
}
```

CHAPTER 5

Configuring Basic System Management

This chapter includes the following topics:

Configuring Basic Router or Switch Properties

When you configure the router initially, you must configure the basic properties of a router, such as the router's hostname, IP addresses, and the name of the domain in which the router is located.

To configure basic router properties:

1. Configure the router's hostname.

   See "Configuring the Hostname of the Router or Switch" on page 62

2. Map the router's hostname to IP addresses.

   See "Mapping the Name of the Router to IP Addresses" on page 63.

3. Configure an ISO system identifier for the router.

   See "Configuring an ISO System Identifier for the Router" on page 63.

4. Configure the router's domain name.

   See "Configuring the Domain Name for the Router or Switch" on page 64.

Related Documentation

- Example: Configuring the Name of the Router, IP Address, and System ID on page 64
- Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine on page 23
- Configuring the Junos OS the First Time on a Router with Dual Routing Engines on page 27
- Configuring the Physical Location of the Router or Switch on page 69
- Configuring a Backup Router on page 66

Configuring the Hostname of the Router or Switch

To configure the name of the router or switch, include the **host-name** statement at the **[edit system]** hierarchy level:

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

The name value must be less than 256 characters.

Related Documentation

- Example: Configuring the Name of the Router, IP Address, and System ID on page 64
- Example: Configuring the Name of the Switch, IP Address, and System ID
- Configuring Basic Router or Switch Properties on page 62
- Mapping the Name of the Switch to IP Addresses
- host-name

Mapping the Name of the Router 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.

Related Documentation

- Configuring Basic Router or Switch Properties on page 62
- Example: Configuring the Name of the Router, IP Address, and System ID on page 64
- Example: Configuring a Router Name and Domain Name on page 263

Configuring an ISO System Identifier for the Router

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).

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.

Related Documentation

- Configuring Basic Router or Switch Properties on page 62
- Example: Configuring the Name of the Router, IP Address, and System ID on page 64

Example: Configuring the Name of the Router, IP Address, and System ID

The following example shows how to 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;
    }
  }
}
```

Related Documentation

- Configuring Basic Router or Switch Properties on page 62

Configuring the Domain Name for the Router or Switch

For each router or switch, you should configure the name of the domain in which the router or switch 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;
```

The following example shows how to configure the domain name:

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

Related Documentation

- **domain-name on page 343**
- domain-name

- Example: Configuring the Domain Name for the Router or Switch on page 65

Example: Configuring the Domain Name for the Router or Switch

The following example shows how to configure the router or switch domain name:

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

Related Documentation

- domain-name
- Configuring the Domain Name for the Router or Switch on page 64

Configuring the Domains to Search When a Router or Switch Is Included in Multiple Domains

If your router or switch 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 six domain names, with a total of up to 256 characters.

The following example shows how to configure two domains to be searched:

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

Related Documentation

- Example: Configuring the Domain Name for the Router or Switch on page 65
- Configuring a DNS Name Server for Resolving a Hostname into Addresses on page 65

  Configuring a DNS Name Server for Resolving a Hostname into Addresses

Configuring a DNS Name Server for Resolving a Hostname into Addresses

To have the router or switch 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;
```

```
}
```

The following example shows how to 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;
  }
}
```

Related Documentation

- Configuring the Domains to Search When a Router or Switch Is Included in Multiple Domains on page 65
- **name-server on page 386**

Configuring a Backup Router

When a router or switch is booting, the routing protocol process (rpd) is not running; therefore, the router or switch has no static or default routes. To allow the router or switch to boot and to ensure that the router or switch 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 or switch (that is, on the same subnet).

To achieve network reachability while loading, configuring, and recovering the router or switch, but without the risk of installing a default route in the forwarding table, include the **destination** option. Specify the address in the format ***network/mask-length*** so that the entire network is reachable through the backup router.

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.

NOTE: **The routes 0.0.0.0/0 or ::/0 should not be used as a destination address in the backup router configuration. You must include a proper subnet range of /8 or higher in the destination address.**

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.

The following topics describe how to configure a backup router running IPv4 and IPv6, respectively:

Configuring a Backup Router Running IPv4

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>;
```

The following example shows how to configure a backup router running IPv4 and have its address remain in the routing and forwarding tables:

NOTE: The Routing Engine on the backup router only supports 16 destinations addresses. If you configure more than 16 destination addresses, the Junos OS ignores destination addresses after the sixteenth address and displays a commit-time warning message to this effect.

```
[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;
    }
  }
}
```

Configuring a Backup Router Running IPv6

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>";
```

The following example shows how to configure a backup router running IPv6 and have its address remain in the routing and forwarding tables:

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

```
            static {
               route abcd::/48 {
                  next-hop 8:3::1;
                  retain;
               }
            }
         }
      }
```

Related Documentation

- Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine on page 23
- Configuring the Junos OS the First Time on a Router with Dual Routing Engines on page 27

Configuring Automatic Mirroring of the CompactFlash Card on the Hard Disk Drive

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 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 feature is not available on the J Series routers.

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

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

To configure the mirroring of the CompactFlash card 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.

Related Documentation

- Using Junos OS to Specify the Number of Configurations Stored on the CompactFlash Card on page 245
- Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine on page 23

Configuring the Physical Location of the Router or Switch

To configure the physical location of the router or switch, you can configure the following options for the **location** statement at the **[edit system]** hierarchy level:

- **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.

The following example shows how to configure the physical location of the router or switch:

```
[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;
}
```

Related Documentation

- Configuring Basic Router or Switch Properties on page 62

Configuring the Root Password

The Junos OS is preinstalled on the router or switch. When the router or switch is powered on, it is ready to be configured. Initially, you log in 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 can commit a configuration, but you are *not* able to log in as superuser and gain root level access to the router or switch.

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.

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
        20740496252839038203869014158453496417001961060835872296
        15634757491827360336127644187426594689320773910834481012
        68312595772262546166799927831612350043866091586628382248
        97467326056611921489539813965561563786211940327687806538
        16960202749164163735913269396344008443 boojum@juniper.net"; #
```

```
    SECRET-DATA
}
```

Junos-FIPS software 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 or switch, 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.

Related Documentation

- Example: Configuring the Root Password on page 71
- Example: Configuring a Plain-Text Password for Root Logins on page 71
- Example: Configuring SSH Authentication for Root Logins on page 72
- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 75
- Recovering the Root Password on page 124

Example: Configuring the Root Password

The following example shows how to configure the root password:

```
[edit]
user@switch# set system root-authentication encrypted-password
  "$1$14c5.$sBopasddsdfs0"
[edit]
user@switch# show
system {
  root-authentication {
    encrypted-password "$1$14c5.$sBopasddsdfs0";
  }
}
```

Related Documentation

- Configuring the Root Password on page 70
- Example: Configuring a Plain-Text Password for Root Logins on page 71
- Configuring the Root Password

Example: Configuring a Plain-Text Password for Root Logins

The following example shows how to set a plain-text password for root logins:

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

```
system {
  root-authentication {
    encrypted-password "$1$14c5.$sBopasddsdfs0";
  }
}
```

Related Documentation

- Configuring the Root Password on page 70

Example: Configuring SSH Authentication for Root Logins

The following example shows how to 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";
}
```

Related Documentation

- Configuring the Root Password on page 70
- Special Requirements for Junos OS Plain-Text Passwords on page 72

Special Requirements for Junos OS Plain-Text Passwords

The Junos OS has special requirements when you create plain-text passwords on a router or switch. Table 5 on page 72 shows the default requirements.

Table 5: Special Requirements for Plain-Text Passwords

Junos OS	Junos-FIPS
The password must be between 6 and 128 characters long.	FIPS passwords must be between 10 and 20 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.	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).

You can change the requirements for plain-text passwords.

Junos OS supports the following five character classes for plain-text passwords:

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

Control characters are not recommended.

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]**

  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 you omit the **change-type** option, Junos-FIPS plain-text passwords are checked for character sets and Junos OS 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 you do not use the **minimum-changes** statement, character sets are not checked for Junos OS. If the **change-type** statement is configured for the **character-set**option, then the **minimum-changes** value must be **5** or less, because the Junos OS only supports five character sets.

  The **format** statement specifies the hash algorithm (**md5**, **sha1** or **des**) for authenticating plain-text passwords. This statement is optional. For Junos OS, 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 OS 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 OS 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 OS 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;
}
```

Related Documentation

- Changing the Requirements for Junos OS Plain-Text Passwords on page 74
- Configuring the Root Password on page 70
- Changing the Requirements for Junos OS Plain-Text Passwords
- Configuring the Root Password

Changing the Requirements for Junos OS Plain-Text Passwords

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;
}
```

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

Related Documentation

- Special Requirements for Junos OS Plain-Text Passwords on page 72
- Configuring the Root Password on page 70
- Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 75

Example: Changing the Requirements for Junos OS Plain-Text Passwords

The following example shows how to set the minimum password length to 12 characters and the maximum length to 22 characters:

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

Related Documentation

- Changing the Requirements for Junos OS Plain-Text Passwords on page 74
- Changing the Requirements for Junos OS Plain-Text Passwords

Configuring Multiple Routing Engines to Synchronize Committed Configurations Automatically

If your router or switch 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.

Related Documentation

- Junos OS Commit Model for Router or Switch Configuration on page 8

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 enables 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 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 compress the configuration files (this is the default) to minimize the amount of disk space that they require.**

- If you want 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
```

- 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-compression-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# commit
commit complete
user@host# commit
commit complete
```

Related Documentation

- Junos OS Commit Model for Router or Switch Configuration on page 8
- compress-configuration-files

CHAPTER 6

Configuring User Access

This chapter includes the following topics:

Junos OS Login Classes Overview

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

- Access privileges that users have when they are logged in to the router or switch
- 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 and then apply one login class to an individual user account.

The Junos OS contains a few predefined login classes, which are listed in Table 6 on page 78. The predefined login classes cannot be modified.

Table 6: Predefined System Login Classes

Login Class	Permission Flag Set
operator	clear, network, reset, trace, and view
read-only	view
superuser or **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 OS appends **-local** to the login class name. The following message also appears:

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

- 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

Related Documentation

- Defining Junos OS Login Classes on page 78
- Defining Junos OS Login Classes

Defining Junos OS Login Classes

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 {
   access-end;
   access-start;
   allow-commands "regular-expression";
   allow-configuration-regexps "regular expression 1" “regular expression 2”;
   allowed-days;
   deny-commands "regular-expression";
   deny-configuration-regexps "regular expression 1" “regular expression 2” ...;
   idle-timeout minutes;
   permissions [ permissions ];
}
```

Related Documentation

- Junos OS Login Classes Overview on page 78
- Junos OS User Accounts Overview on page 79
- Example: Creating Login Classes on page 265
- Configuring the Junos OS to Display a System Login Announcement on page 240
- Disabling Junos OS Processes on page 240
- Using Junos OS to Configure Logical System Administrators on page 242

Junos OS User Accounts Overview

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 “Junos OS User Authentication Methods” on page 51.) 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.

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 “Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies” on page 100.

- 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 OS 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 SSH authentication, you can also copy the contents of an SSH keys file into the configuration.

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
    20740496252839038203869014158453496417001961060835872296156З
    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 70.

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.

Related Documentation

- Configuring Junos OS User Accounts on page 81
- Junos OS Login Classes Overview on page 78

Configuring Junos OS User Accounts

User accounts provide one way for users to access the router or switch. 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";
    }
}
```

Related Documentation

- Example: Configuring User Accounts on page 81
- Example: Configuring User Login Accounts on page 265
- Junos OS User Accounts Overview on page 79
- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 82

Example: Configuring User Accounts

The following example shows how to 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;
            }
        }
    }
```

Related Documentation

- Junos OS User Accounts Overview on page 79
- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 82

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

You can limit the number of 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;
   maximum-time seconds
   minimum-time seconds;
}
```

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.
- **maximum-time *seconds***—Maximum length of time, in seconds, that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured **maximum-time**, the connection is closed. The range is from 20 through 300 seconds, and the default is 120 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.

Related Documentation

- Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions on page 83
- Configuring Junos OS User Accounts on page 81

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

The following example shows how to limit the user to four attempts when the user enters 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 {
        }
    }
}
```

NOTE: This sample only shows the portion off the [edit system login] hierarchy being modified.

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 82
- **login on page 377**
- login

Configuring Time-Based User Access

The Junos OS enables you to configure time-based restrictions for user access to log in to a device. This is useful for restricting the time and duration of user logins for all users belonging to a login class. You can specify the days of the week when users can log in, the access start time, and the access end time.

- To configure user access on specific days of the week, without any restrictions on the duration of login, include the **allowed-days** statement only.

  ```
  [edit system]
  login {
      class class-name {
          allowed-days [ days-of-the-week ];
      }
  ```

- To configure user access on all the days of the week for a specific duration, include the **access-start** and **access-end** statements only.

  ```
  [edit system]
  login {
      class class-name {
          access-start HH:MM;
          access-end HH:MM;
      }
  }
  ```

- To configure user access on specific days of the week for a specified duration, include the **allowed-days**, **access-start**, and **access-end** statements.

```
[edit system]
login {
    class class-name {
        allowed-days [ days-of-the-week ];
        access-start HH:MM;
```



```
        access-end HH:MM;
    }
}
```

Specify the start time and end time in ***HH:MM*** (24-hour) format, where ***HH*** represents the hours and ***MM*** represents the minutes.

NOTE: Access start time and end time that spans across 12:00 AM on a specified day results in the user having access until the next day, even if the access day is not explicitly configured. For instance, the following configuration results in the user having access until 6:00 AM on Tuesday and Thursday, although the **allowed-days** statement specifies access only on Monday and Wednesday:

```
[edit system]
login {
    class operator-night-shift {
        allowed-days [ monday wednesday ];
        access-start 2000;
        access-end 0600;
    }
}
```

Related Documentation

- Examples: Configuring Time-Based User Access on page 85
- Defining Junos OS Login Classes on page 78
- **access-end on page 295**
- **access-start on page 295**
- **allowed-days on page 298**
- access-end
- access-start
- allowed-days

Examples: Configuring Time-Based User Access

The following example shows how to configure user access for the **operator-round-the-clock-access** login class from Monday through Friday without any restriction on access time or duration of login:

```
[edit system]
login {
    class operator-round-the-clock-access {
        allowed-days [ monday tuesday wednesday thursday friday ];
    }
```

The following example shows how to configure user access for the **operator-day-shift** login class on Monday, Wednesday, and Friday from 8:30 AM to 4:30 PM:


```
[edit system]
login {
  class operator-day-shift {
    allowed-days [ monday wednesday friday ];
    access-start 0830;
    access-end 1630;
  }
}
```

Alternatively, you can also specify the login start time and end time for the **operator-day-shift** login class to be from 8:30 AM to 4:30 PM in the following format:

```
[edit system]
login {
  class operator-day-shift {
    allowed-days [ monday wednesday friday ];
    access-start 08:30am;
    access-end 04:30pm;
  }
}
```

The following example shows how to configure user access for the **operator-day-shift-all-days-of-the-week** login class to be on all days of the week from 8:30 AM to 4:30 PM:

```
[edit system]
login {
  class operator-day-shift-all-days-of-the-week {
    access-start 0830;
    access-end 1630;
  }
}
```

Related Documentation

- Configuring Time-Based User Access on page 84

Junos-FIPS Crypto Officer and User Accounts Overview

Junos-FIPS defines a restricted set of user roles. Unlike the Junos OS, which enables 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.

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.

Related Documentation

- Junos OS User Accounts Overview on page 79

Junos OS Access Privilege Levels Overview

Each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with them. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more *permission flags*.

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.

The following sections provide additional information about permissions:

- Junos OS Login Class Permission Flags on page 87
- Allowing or Denying Individual Commands for Junos OS Login Classes on page 90

Junos OS Login Class Permission Flags

The **permissions** statement specifies one or more of the permission flags listed in Table 7 on page 87. 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 of permissions control for individual parts of the configuration are:

- "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 7 on page 87 lists the Junos OS login class permission flags that you can configure by including the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level.

Table 7: Login Class Permission Flags

Permission Flag	Description
access	Can view the access configuration in configuration mode and with the **show configuration** operational mode command.

Table 7: Login Class Permission Flags *(continued)*

Permission Flag	Description
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** operational mode 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 by using the **clear** commands.
configure	Can enter configuration mode by using the **configure** command.
control	Can perform all control-level operations—all operations configured with the **-control** permission flags.
field	Can view field debug commands. Reserved for 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 or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must authenticate itself to the Junos OS as an administrative user. That account must have **flow-tap-operation** permission. NOTE: The **flow-tap-operation** option is not included in the **all** permissions flag.
interface	Can view the interface configuration in configuration mode and with the **show configuration** operational mode command.

Table 7: Login Class Permission Flags *(continued)*

Permission Flag	Description
interface-control	Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels: • **[edit chassis]** • **[edit class-of-service]** • **[edit groups]** • **[edit forwarding-options]** • **[edit interfaces]**
maintenance	Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell by using the **su root** command, and can halt and reboot the router by using the **request system** commands.
network	Can access the network by using the **ping**, **ssh**, **telnet**, and **traceroute** commands.
pgcp-session-mirroring	Can view **pgcp** session mirroring configuration.
pgcp-session-mirroring-control	Can modify **pgcp** session mirroring configuration.
reset	Can restart software processes by 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 can 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.

Table 7: Login Class Permission Flags *(continued)*

Permission Flag	Description
security-control	Can view and configure security information at the **[edit security]** hierarchy level.
shell	Can start a local shell on the router or switch by using 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 can 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 and configure trace file properties.
trace-control	Can modify trace file settings and configure trace file properties.
view	Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view secret configuration.
view-configuration	Can view all of the configuration (excluding secrets).

Allowing or Denying Individual Commands for Junos OS Login Classes

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.

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 ... cmd*n***), you can specify each command as a separate expression. This new syntax is valid for **allow-configuration-regexps** and **deny-configuration-regexps**, **allow-commands** and **deny-commands**, and all user permission bits.
- Users cannot issue the **load override** command when specifying an extended regular expression. Users can only issue the **merge**, **replace**, and **patch** configuration commands.
- If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by the **deny-commands**. For example, if you include **allow-commands "request system software add"** and **deny-commands "request system software add"**, the login class user is allowed to install software using the **request system software add** command.
- Regular expressions for **allow-commands** and **deny-commands** can also include the **commit**, **load**, **rollback**, **save**, **status**, and **update** commands.
- If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

  For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **allow-commands**.

  Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **deny-commands**.

Related Documentation

- Configuring Access Privilege Levels on page 92

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.

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 ];
```

Related Documentation

- Example: Configuring Access Privilege Levels on page 92
- Junos OS Access Privilege Levels Overview on page 87
- Specifying Access Privileges for Junos OS Operational Mode Commands on page 92
- Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 96
- Specifying Access Privileges for Junos OS Configuration Mode Hierarchies
- **permissions on page 401**
- permissions

Example: Configuring Access Privilege Levels

Create two access privilege classes on the router or switch, 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 ];
      }
   }
}
```

Related Documentation

- Configuring Access Privilege Levels on page 92

Specifying Access Privileges for Junos OS Operational Mode Commands

You can specify extended regular expressions by using the **allow-commands** and **deny-commands** statements to define a user's access privileges to individual operational mode commands. Doing so takes precedence over login class permissions bit set for a user. You can include one **deny-commands** and one **allow-commands** statement in each login class.

To explicitly provide use of 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 access to an individual operational mode command that would otherwise be supported, 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 the expression in quotation marks. Regular expressions are not case-sensitive.

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

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*.

Explicitly providing access to operational mode commands using the **allow-commands** statement adds to the regular permissions set using the **permissions** statement. Likewise, explicitly denying access to operational mode commands using the **deny-commands** statement removes permissions for the specified commands from the default permissions provided by the **permissions** statement.

For example, if a login class has permissions **view** and the **allow-commands** statement includes the **request system software add** command, the specified login class user can install software, in addition to the permissions specified by the **view** permissions flag. Likewise, if a login class has permissions **all** and the **deny-commands** statement includes the **request system software add** command, the specified login class user can perform all operations allowed by the **all** permissions flag, except installing software using the **request system software add** command.

If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by **deny-commands**. For example, if you include **allow-commands "request system software add"** and **deny-commands "request system software add"**, the login class user is allowed to install software using the **request system software add** command.

If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **allow-commands**.

Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **deny-commands**.

Anchors are required when specifying complex regular expressions with **allow-commands** or **deny-commands** statements. For example, when specifying multiple commands using the pipe (|) symbol for **allow-commands**, the following syntax is incorrect: **allow-commands = "(monitor.*)|(ping.*)|(show.*)|(exit)"** . Instead, you must specify the expression using the following syntax: **allow-commands** = **"(^monitor) | (^ping) | (^show) | (^exit)"** OR **allow-commands ="^(monitor | ping | show | exit)"**

Related Documentation

- Example: Configuring Access Privileges for Operational Mode Commands on page 95
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands on page 94
- **allow-commands on page 296**
- **deny-commands on page 331**
- allow-commands
- deny-commands

Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands

Use extended regular expressions to specify which operational mode commands are denied or allowed. Table 8 on page 94 lists common regular expression operators that can be used in the operational mode commands. Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2.

Table 8: 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**).
^	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.

Table 8: Common Regular Expression Operators to Allow or Deny Operational Mode Commands *(continued)*

Operator	Match
[ ]	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";
```

Related Documentation

- Specifying Access Privileges for Junos OS Operational Mode Commands on page 92

Example: Configuring Access Privileges for Operational Mode Commands

The following example shows how to configure access privileges for different login classes for individual operational mode commands:

```
[edit]
system {
  # This login class has operator privileges and the additional ability
    # to reboot the router.
    login {
    # This login class has operator privileges and the additional ability to reboot the
    # router or switch.
    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” .
    # This login class has operator privileges
      # but cannot 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";
        }
    }
}
```

Related Documentation

- Specifying Access Privileges for Junos OS Operational Mode Commands on page 92

Specifying Access Privileges for Junos OS Configuration Mode Hierarchies

The **allow-configuration-regexps** and **deny-configuration-regexps** statements let you explicitly allow or deny users access privileges to portions of the configuration hierarchy. Each of these statements is added to named login classes and configured with one or more regular expressions to be allowed or denied. The expressions are listed as a string with regular separators, such as white space or other regular expression delimiters. Each login class is assigned to specific users or user IDs.

You can include one **allow-configuration-regexps** and one **deny-configuration-regexps** statement in each login class. Access privileges configured using these statements override permissions set for a login class. If both of these statements are included in a class and there is overlap in the regular expressions defined for them, expressions denied with **deny-configuration-regexps** take precedence over expressions allowed with **allow-configuration-regexps**. You can configure as many regular expressions as needed to be allowed or denied in each class. Although every environment is different, as many as 3000 expressions have been configured in a test environment, and issuing a **show | compare rollback** command has taken only seconds to complete. You can use **allow-configuration-regexps** and **deny-configuration-regexps** configuration privileges statements in the same class with the **allow-commands** and **deny-commands** operational privileges statements.

These statements give the system administrator precise control over who can change specific configurations in the system.

Related Documentation

- Example: Specifying Access Privileges Using Allow or Deny Configuration with Regular Expressions on page 96

Example: Specifying Access Privileges Using Allow or Deny Configuration with Regular Expressions

Requirements

The minimum requirement for this feature is one Juniper Networks J Series, M Series, MX Series, or T Series device running Junos OS Release 11.2 or later, with at least one user assigned to a login class. There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview

The **allow-configuration-regexps** and **deny-configuration-regexps** statements let you explicitly allow or deny users access privileges to portions of the configuration hierarchy. Each of these statements is added to named login classes and configured with one or more regular expressions to be allowed or denied. The expressions are listed as a string with regular separators, such as white space or other regular delimiters. Each login class is assigned to specific users or user IDs.

You can include one **deny-configuration-regexps** and one **allow-configuration-regexps** statement in each login class. Access privileges configured using these statements override permissions set for a login class. If both of these statements are included in a class and there is overlap in the regular expressions defined for them, expressions denied with **deny-configuration-regexps** take precedence over expressions allowed with **allow-configuration-regexps**. You can configure as many regular expressions as needed to be allowed or denied in each class. Although every environment is different, as many as 3000 expressions have been configured in a test environment, and issuing a **show | compare rollback** command took only seconds to complete. You can use **allow-configuration-regexps** and **deny-configuration-regexps** configuration privileges statements in the same class with the **allow-commands** and **deny-commands** operational privileges statements.

These statements give the system administrator precision control over who can change specific configurations in the system.

Configuration

This procedure shows basic steps for setting up configuration access privileges using **allow-configuration-regexps** and **deny-configuration-regexps**.

1. To explicitly allow one or more individual configuration mode hierarchies that would otherwise be denied, include the **allow-configuration-regexps** statement at the **[edit system login class *class-name*]** hierarchy level, configured with the regular expressions to be allowed:

   [edit system login class *class-name*]
   user@host# **set allow-configuration-regexps "*regular expression 1*" "*regular expression 2*" "*regular expression 3*" "*regular expression 4*" ...**

2. To explicitly deny one or more individual configuration hierarchies that would otherwise be allowed, include the **deny-configuration-regexps** statement at the **[edit system login class *class-name*]** hierarchy level, configured with the regular expressions to be denied:

   [edit system login class *class-name*]

user@host# **set deny-configuration-regexps "*regular expression 1*" "*regular-expression 2*" "*regular expression 3*" "*regular expression 4*"...**

3. Assign the login class to one or more users:

   [edit system login]
   user@host# **set user *username* class *class-name***

4. Commit your changes. Users assigned this login class have the permissions you have set for the class.

Examples Using Allow or Deny Configurations with Regular Expressions

Purpose

This section provides examples of access privilege configurations to give you ideas for creating configurations appropriate for your system. You can use combinations of privilege statements for configuration access and for operational mode commands to give precise control over classes of access privileges.

Allow Configuration Changes

The following example login class lets the user make changes at the **[edit system services]** hierarchy level and issue configuration mode commands (such as **commit**), in addition to the permissions specified by the **configure** permissions flag, which allows the user to enter configuration mode using the **configure** command.

[edit system login class *class-name*]
user@host# **set permissions configure view view-configuration**
user@host# **set allow-configuration-regexps "system services"**

Deny Configuration Changes

The following example login class lets the user perform all operations allowed by the **all** permissions flag. However, it denies modifying the configuration at the **[edit system services]** hierarchy level.

[edit system login class *class-name*]
user@host# **set permissions all configure view view-configuration**
user@host# **set deny-configuration-regexps "system services"**

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 edit the configuration or issue commands (such as **commit**) at the **system login class** or the **system services** hierarchy levels:

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

Allow and Deny Configuration Changes

The following example login class lets the user perform all operations allowed by the **all** permissions flag, and explicitly grants configuration access to **[system "interfaces .* unit .* family inet address .*" protocols]**. However, the user is denied configuration access to the SNMP hierarchy level.

NOTE: You can use the * wildcard character when denoting regular expressions. However, it must be used as a portion of a regular expression. You cannot use [*] or [.*] alone.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set allow-configuration-regexps system "interfaces .* unit .* family inet
   address .*" protocols
user@host# set deny-configuration-regexps snmp
```

Allow and Deny Multiple Configuration Changes

The following example login class lets the user perform all operations allowed by the **all** permissions flag, and explicitly grants configuration access to multiple hierarchy levels for interfaces. It denies configuration access to the **system** and **protocols** hierarchy levels.

NOTE: You can configure as many regular expressions as needed to be allowed or denied. Regular expressions to be denied take precedence over configurations to be allowed.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set allow-configuration-regexps "interfaces .* description .*" "interfaces .*
   unit .* description .*" "interfaces .* unit .* family inet address .*" "interfaces .* disable"
user@host# set deny-configuration-regexps "system" "protocols"
```

Allow Configuration Changes and Deny Operations Commands

You can combine allow and deny configuration statements with allow and deny operational commands statements to fine-tune access privileges. The following example login class uses a combination of the **deny-commands** operational permissions statement and the **allow-configuration-regexps** configuration permissions statement to let the user configure and commit changes to the OSPF and BGP protocols. However, this class of user cannot issue the **show system statistics** or the **show bgp summary** commands.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set deny-commands "(show system statistics)|(show bgp summary)"
user@host# set allow-configuration-regexps "protocols ospf|bgp"
```

The following shows permissions set for individual configuration mode hierarchies:

```
[edit]
system {
   login { # This login class has operator privileges and the additional ability to edit
      # configuration at the system services hierarchy level.
      class only-system-services {
         permissions [ configure ];
         allow-configuration "system services";
```



```
        }
        # services commands.
        class all-except-system-services { # This login class has operator privileges but
          # cannot edit any system services configuration.
          permissions [ all ];
          deny-configuration "system services";
        }
      }
    }
```

Verifying Access Privileges

To verify that you have set the access privileges correctly:

1. Configure a login class and commit the changes.
2. Assign the login class to a *username*.
3. Log in as the *username* assigned with the new login class.
4. Attempt to perform the configurations that have been allowed or denied.
   - You should be able to perform configuration changes to hierarchy levels and regular expressions that have been allowed.
   - You should not be able to perform configuration changes to hierarchy levels and regular expressions that have been denied.
   - Denied expressions should take precedence over allowed expressions.
   - Any allowed or denied expressions should take precedence over any permissions granted with the **permissions** statement.

Related Documentation

- Example: Configuring Access Privilege Levels on page 92
- Junos OS Access Privilege Levels Overview on page 87
- Specifying Access Privileges for Junos OS Operational Mode Commands on page 92

Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies

Use extended regular expressions to specify which configuration mode hierarchies are denied or allowed. You specify these regular expressions in the **allow-configuration-regexps** and **deny-configuration-regexps** 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 or switch.

Table 9 on page 101 lists common regular expression operators that you can use for allowing or denying commands for configuration mode commands.

Command regular expressions implement the extended (modern) regular expressions, as defined in POSIX 1003.2.

Table 9: Configuration Mode Hierachies—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**).
^	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 " ".

Related Documentation

- Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 96
- Specifying Access Privileges for Junos OS Configuration Mode Hierarchies

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 or switch, even if that session is idle. To close idle sessions automatically, you must 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, unless the user is running telnet or monitoring interfaces using the **monitor interface** or **monitor traffic** command.

Related Documentation

- Defining Junos OS Login Classes on page 78
- **idle-timeout on page 363**
- idle-timeout

Configuring CLI Tips

The Junos OS CLI provides the option of configuring CLI tips for the user. 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.

Related Documentation

- CLI User Interface Overview
- Defining Junos OS Login Classes on page 78
- login-tip

CHAPTER 7

Configuring System Authentication

This chapter includes the following topics:

Configuring RADIUS Authentication

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure RADIUS authentication are:

Configuring RADIUS Server Details

To use RADIUS authentication on the router or switch, 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 or switch must match that used by the server.

Optionally, you can specify the amount of time that the local router or switch waits to receive a response from a RADIUS server (in the **timeout** statement) and the number of times that the router or switch attempts to contact a RADIUS authentication server (in the **retry** statement). By default, the router or switch waits 3 seconds. You can configure this to be a value from 1 through 90 seconds. By default, the router or switch retries connecting to the server 3 times. You can configure this to be a value 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 “Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 112.

Configuring MS-CHAPv2 for Password-Change Support

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch 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.
- Set the first tried option in the authentication order to RADIUS server.

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;
```

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;
    }
  }
}
```

Specifying a Source Address for the Junos OS to Access External RADIUS Servers

You can specify which source address the Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You can also specify which source address the Junos OS uses when contacting a RADIUS server for sending accounting information.

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 or switch interfaces.

NOTE: **You can configure the Junos OS to select a fixed address as the source address for locally generated IP packets.**

Related Documentation

- Example: Configuring RADIUS Authentication on page 264
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 122
- Juniper Networks Vendor-Specific RADIUS Attributes on page 106
- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 112
- Example: Configuring RADIUS Template Accounts on page 266

- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 115
- Junos OS User Authentication Methods on page 51
- Example: Configuring RADIUS System Accounting on page 248

Juniper Networks Vendor-Specific RADIUS Attributes

The Junos OS 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 10 on page 106 lists the Juniper Networks VSAs you can configure.

Table 10: 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 enables 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 "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands" on page 94.
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 "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands" on page 94.
Juniper-Allow-Configuration	Contains an extended regular expression that enables 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 "Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 100.

Table 10: Juniper Networks Vendor-Specific RADIUS Attributes *(continued)*

Name	Description	Type	Length	String
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 "Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 100.
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.
Juniper-User-Permissions	Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets. NOTE: When the **Juniper-User-Permissions** attribute is configured to grant the Junos OS **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 the 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.	10	≥3	One or more octets containing printable ASCII characters. 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 7 on page 87.

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

Related Documentation

- Configuring RADIUS Authentication on page 103
- Configuring RADIUS Authentication

Configuring TACACS+ Authentication

TACACS+ authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure TACACS+ configuration are:

Configuring TACACS+ Server Details

To use TACACS+ authentication on the router or switch, 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 or switch 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 or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch 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 OS will be unable to communicate with that TACACS+ server.

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

On a TX Matrix router, 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 router, 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 "Overview of Template Accounts for RADIUS and TACACS+ Authentication" on page 112.

Specifying a Source Address for the Junos OS to Access External TACACS+ Servers

You can specify which source address the Junos OS uses when accessing your network to contact an external TACACS+ server for authentication. You can also specify which source address the Junos OS 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 or switch 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 or switch interfaces.

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 108.

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**.

The following example shows how to 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 Juniper Networks Vendor-Specific TACACS+ Attributes

The Juniper Networks Vendor-Specific TACACS+ Attributes enable you to configure access privileges for users on a TACACS+ server. They are specified in the TACACS+ server configuration file on a per-user basis. The Junos OS 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 OS 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-regexps = "<allow-configuration-regex>"
   deny-commands = "<deny-commands-regex>"
   deny-configuration-regexps = "<deny-configuration-regex>"
}
```

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

Related Documentation

- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 122
- Juniper Networks Vendor-Specific TACACS+ Attributes on page 111
- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 112
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 115
- Junos OS User Authentication Methods on page 51

Juniper Networks Vendor-Specific TACACS+ Attributes

The Junos OS supports the configuration of Juniper Networks TACACS+ vendor-specific attributes (VSAs). These VSAs are encapsulated in a TACACS+ vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 11 on page 111 lists the Juniper Networks VSAs you can configure.

Table 11: 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 enables 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 8 on page 94.
allow-configuration-regexps	Contains an extended regular expression that enables 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 "Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 100.
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 8 on page 94.
deny-configuration-regexps	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 9 on page 101.

Table 11: Juniper Networks Vendor-Specific TACACS+ Attributes *(continued)*

Name	Description	Length	String
user-permissions	Contains information the server uses to specify user permissions. 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.	≥3	One or more octets containing printable ASCII characters. See Table 7 on page 87.

Related Documentation

- Configuring Juniper Networks Vendor-Specific TACACS+ Attributes on page 110
- Configuring TACACS+ Authentication

Overview of 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.

Related Documentation

- Configuring Remote Template Accounts for User Authentication on page 112
- Configuring Local User Template Accounts for User Authentication on page 113

Configuring Remote Template Accounts for User Authentication

By default, the Junos OS uses remote template accounts for user authentication when:

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

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** statements in the authentication server configuration file.

Related Documentation

- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 112
- **user (Access) on page 464**
- user (Access)

Configuring Local User Template Accounts for User Authentication

You use local user template accounts when you need different types of templates for authentication. 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 OS 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 OS, 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 OS 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.

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;
}
```

This example configures 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;
      }
   }
}
```

```
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, the switch applies the sales local user template. When login users Harold and Jim are authenticated, the switch applies the engineering local user template.

Related Documentation

- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 112
- **user (Access) on page 464**
- user (Access)

Using Regular Expressions on a RADIUS or TACACS+ Server 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 RADIUS or TACACS+ attributes in your authentication server configuration.

You can specify **allow-configuration**, **deny-configuration**, **allow-commands**, or **deny-commands** in a single extended regular expression, enclosing multiple commands in parentheses and separating them using the pipe symbol. For example, you can specify multiple **allow-commands** parameters using: **allow-commands= (cmd1 | cmd2 | cmd*n*)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

On a RADIUS or TACACS+ server, you can also use a simplified version for regular expressions where you specify each individual expression on a separate line. The simplified version is valid for **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, and **permissions** vendor-specific attributes:

For a RADIUS server, specify the individual regular expressions using the following syntax:

```
Juniper-Allow-Commands+="cmd1"
Juniper-Allow-Commands+="cmd2"
Juniper-Allow-Commands+="cmdn"
Juniper-Deny-Commands+="cmd1"
Juniper-Deny-Commands+="cmd2"
Juniper-Deny-Commands+="cmdn"
Juniper-Allow-Configuration+="regex1"
Juniper-Allow-Configuration+="regex2"
Juniper-Allow-Configuration+="regexn"
Juniper-Deny-Configuration+="regex1"
Juniper-Deny-Configuration+="regex2"
Juniper-Deny-Configuration+="regexn"
Juniper-User-Permissions+="permission-flag1"
Juniper-User-Permissions+="permission-flag2"
Juniper-User-Permissions+="permission-flagn"
```

For a TACACS+ server, specify the individual regular expressions using the following syntax:

```
allow-commands1="cmd1"
allow-commands2="cmd2"
allow-commandsn="cmdn"
deny-commands1="cmd1"
deny-commands2="cmd2"
deny-commandsn="cmdn"
allow-configuration1="regex1"
allow-configuration2="regex2"
allow-configurationn="regexn"
deny-configuration1="regex1"
deny-configuration2="regex2"
deny-configurationn="regexn"
```

```
user-permissions1="permission-flag1"
user-permissions2="permission-flag2"
user-permissionsn="permission-flagn "
```

NOTE:

- Numeric values 1 to *n* in the syntax (for a TACACS+ server) must be unique but need not be sequential. For example, the following syntax is valid:

  ```
  allow-commands1="cmd1"
  allow-commands3="cmd3"
  allow-commands2="cmd2"
  deny-commands3="cmd3"
  deny-commands2="cmd2"
  deny-commands1="cmd1"
  ```

- The limit on the number of lines of individual regular expressions is imposed by the TACACS+ or RADIUS server.
- When you issue the **show cli authorization** command, the command output displays the regular expression in a single line, even if you specify each individual expression on a separate line.

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see "Juniper Networks Vendor-Specific RADIUS Attributes" on page 106 and "Juniper Networks Vendor-Specific TACACS+ Attributes" on page 111.

NOTE: When RADIUS or TACACS+ 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 using the **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, or **permissions** statements. If the final expression has a syntax error, the overall result is an invalid regular expression.

Related Documentation

- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 116

Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

For each login attempt, the Junos OS 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 order is tried if the previous authentication method fails to respond or if the method returns a reject response to the login attempt because of 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 OS consults local password authentication as a last resort.

Using RADIUS or TACACS+ Authentication

You can configure the Junos OS to be both a RADIUS and 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 OS 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 TACACS+ 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 because of 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 or switch 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 or switch using their local username 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 method is tried if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response because of 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 tried only if all configured

authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response because of an incorrect username or password.

Order of Authentication Attempts

Table 12 on page 118 describes how the **authentication-order** statement at the **[edit system]** hierarchy level determines the procedure that the Junos OS uses to authenticate users for access to a router or switch:

Table 12: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
authentication-order radius;	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS server is available but authentication is rejected, deny access. 4. If RADIUS servers are not available, try password authentication. 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. 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. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ server is available but authentication is rejected, deny access. 6. If both RADIUS and TACACS+ servers are not available, try password authentication. 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 12: Order of Authentication Attempts *(continued)*

Syntax	Order of Authentication Attempts
authentication-order [radius tacplus password];	1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 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. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ server is available but authentication is rejected, deny access. 4. If TACACS+ servers are not available, try password authentication. 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. 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. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS server is available but authentication is rejected, deny access. 6. If both TACACS+ and RADIUS servers are not available, try password authentication. 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 12: Order of Authentication Attempts *(continued)*

Syntax	Order of Authentication Attempts
authentication-order [tacplus radius password];	1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 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. 2. If the authentication is accepted, grant access. 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.

In a routing matrix based on a TX Matrix router or a TX Matrix Plus router, the authentication order must be configured only at the configuration groups **re0** and **re1**. The authentication order must not be configured under the **[edit system]** hierarchy on the TX Matrix or TX Matrix Plus router. This is because the authentication order for the routing matrix is controlled on the switch-card chassis (or TX Matrix router) or switch-fabric chassis (or TX Matrix Plus router) only.

Related Documentation

- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 112
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 122
- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 82
- Limiting the Number of User Login Attempts for SSH and Telnet Sessions
- Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 121

Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

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.

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 or switch 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 OS enforces a limit on the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—might fail to authenticate a client when this limit is exceeded. If it fails, the authentication sequence is reinitiated by the router or switch until authentication succeeds and the link is brought up. However, if the RADIUS servers are not available and if additional authentication methods such as **tacplus** or **password** are configured along with **radius**, the next authentication method is tried.

The following example shows how to configure **radius** and **password** authentication:

```
[edit system]
user@switch# authentication-order [ radius password ];
```

The following example shows how to delete the **radius** statement from the authentication order:

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


The following example shows how to insert the **tacplus** statement after the **radius** statement:

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

Related Documentation

- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 116
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 115
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 122
- **authentication-order on page 309**

Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

If the RADIUS server is not available, the user is authe

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If the If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see “Using Local Password Authentication” on page 117.

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 privileges associated with 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 “Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 112.

When a user logs into a device, the user’s login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

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 OS 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.

Related Documentation

- Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 121

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.
4. Plug the RJ-45–to–DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the 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**

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. After you have finished configuring the password, 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**

Related Documentation

- Configuring the Root Password on page 70

CHAPTER 8

Configuring Time

This chapter includes the following topics:

Modifying the Default Time Zone for a Router or Switch Running Junos OS

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 (GMThour-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 **0**. You can configure this 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 or switch, you must reboot the router or switch.

The following example shows how to change the current time zone to **America/New_York**:

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

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

Related Documentation

- NTP Overview on page 128
- Setting a Custom Time Zone on Routers or Switches Running Junos OS on page 136

NTP Overview

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.

In Junos OS Release 11.2 or later, NTP supports IPv4 VPN routing and forwarding (VRF) requests. This enables an NTP server running on a provider edge (PE) router to respond to NTP requests from a customer edge (CE) router. As a result, a PE router can process any NTP request packet coming from different routing instances.

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 or hostname of an NTP server.

Related Documentation

- Synchronizing and Coordinating Time Distribution Using NTP on page 129
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 267

Synchronizing and Coordinating Time Distribution Using NTP

Using NTP to synchronize and coordinate time distribution in a large network involves these tasks:

1. Configuring NTP on page 129
2. Configuring the NTP Boot Server on page 129
3. Specifying a Source Address for an NTP Server on page 129

Configuring NTP

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

```
[edit system]
ntp {
  authentication-key number type type value password;
  boot-server (address | hostname);
  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 ];
}
```

Configuring the NTP Boot Server

When you boot the router or switch, 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 or switch uses to determine the time when the router or switch 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 or switch'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 | hostname);
```

Specify the address of the network server. You must specify an IP address or 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 or switch interfaces.

NOTE: If a firewall filter is applied on the loopback interface, ensure that the **source-address** specified for the NTP server at the **[edit system ntp]** hierarchy level is explicitly included as one of the match criteria in the firewall filter. This enables the Junos OS to accept traffic on the loopback interface from the specified source address.

The following example shows a firewall filter with the source address **10.0.10.100** specified in the **from** statement included at the **[edit firewall filter *firewall-filter-name*]** hierarchy:

```
[edit firewall filter Loopback-Interface-Firewall-Filter]
term Allow-NTP {
  from {
    source-address {
      172.17.27.46/32; // IP address of the NTP server
      10.0.10.100/32; // Source address specified for the NTP server
      }
    then accept;
  }
}
```

If no **source-address** is configured for the NTP server, include the primary address of the loopback interface in the firewall filter.

Related Documentation

- NTP Overview on page 128
- NTP Time Server and Time Services Overview on page 131
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 267

NTP Time Server and Time Services Overview

When configuring the Network Time Protocol (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 or switch to operate in one of the following modes:

- Client mode—In this mode, the local router or switch can be synchronized with the remote system, but the remote system can never be synchronized with the local router or switch.
- Symmetric active mode—In this mode, the local router or switch and the remote system can synchronize with each other. You use this mode in a network in which either the local router or switch 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 or switch 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 or switch is operating as a transmitter.
- Server mode—In this mode, the local router or switch operates as an NTP server.

NOTE: In NTP server mode, the Junos OS supports authentication as follows:

- If the NTP request from the client comes with an authentication key (such as a key ID and message digest sent with the packet), the request is processed and answered based on the authentication key match.
- If the NTP request from the client comes without any authentication key, the request is processed and answered without authentication.

Related Documentation

- Configuring the NTP Time Server and Time Services
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 267

Configuring the NTP Time Server and Time Services

When you use NTP, configure the router or switch to operate in one of the following modes:

- Client mode
- Symmetric active mode
- Broadcast mode
- Server mode

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

Configuring the Router or Switch to Operate in Client Mode

To configure the local router or switch 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 134.

By default, the router or switch 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 134. For information about how to configure an NTP boot server, see “Configuring the NTP Boot Server” on page 129. For information about how to configure the router or switch to operate in server mode, see “Configuring the Router or Switch to Operate in Server Mode” on page 133.

The following example shows how to configure the router or switch 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 or Switch to Operate in Symmetric Active Mode

To configure the local router or switch 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 134.

By default, the router or switch 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 or Switch to Operate in Broadcast Mode

To configure the local router or switch 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 134.

By default, the router or switch 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 or Switch to Operate in Server Mode

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

To configure the local router or switch 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 134.

By default, the router or switch 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 134. For information about how to configure the router or switch to operate in client mode, see “Configuring the Router or Switch to Operate in Client Mode” on page 132.

The following example shows how to configure the router or switch 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;
```

Related Documentation

- NTP Time Server and Time Services Overview on page 131
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 267

Configuring NTP Authentication Keys

Time synchronization can be authenticated to ensure that the local router or switch 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.

Related Documentation

- NTP Time Server and Time Services Overview on page 131
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 267

Configuring the Router or Switch to Listen for Broadcast Messages Using NTP

When you are using NTP, you can configure the local router or switch 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 or switch detects 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.

Related Documentation

- Configuring the Router or Switch to Listen for Multicast Messages Using NTP on page 135
- Configuring the NTP Time Server and Time Services on page 132
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 267

Configuring the Router or Switch to Listen for Multicast Messages Using NTP

When you are using NTP, you can configure the local router or switch 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 or switch receives 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 router or switch 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.

Related Documentation

- Configuring the Router or Switch to Listen for Broadcast Messages Using NTP on page 135
- Configuring the NTP Time Server and Time Services on page 132
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 267

Setting a Custom Time Zone on Routers or Switches Running Junos OS

You can update the time zone database information on routers or switches running Junos OS. This feature simplifies time zone management in devices running Junos OS by allowing for future unforeseen time zone database adjustments. You can configure your router or switch to use a custom time zone database file that you create to meet your requirements by editing an existing time zone database file.

Tasks for setting a custom time zone are:

1. Importing and Installing Time Zone Files on page 136
2. Configuring a Custom Time Zone on page 137

Importing and Installing 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 the configuration:

   [edit]
   # set system time-zone <your-time-zone>
   # commit

5. Verify that the time zone change has taken effect:

   [edit]
   # run show system uptime

Configuring 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 or switch. Compile the time zone archive using the *zic* time zone compiler, which generates *tz* files.

2. Using the CLI, configure the router or switch 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 the router to use imported time zones, the Junos OS default time zones are shown (saved in the directory /usr/share/zoneinfo/).

Related Documentation

- Modifying the Default Time Zone for a Router or Switch Running Junos OS on page 127
- NTP Overview on page 128
- NTP Time Server and Time Services Overview on page 131
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 267
- **use-imported-time-zones on page 464**

CHAPTER 9

Configuring System Log Messages

This chapter includes the following topics:

Junos OS System Log Configuration Overview

The Junos OS generates system log messages (also called *syslog messages*) to record events that occur on the router, 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 router power-down due to excessive temperature

Each system log message identifies the Junos OS process that generated the message and briefly describes the operation or error that occurred. For detailed information about specific system log messages, see the *Junos OS System Log Messages Reference*.

NOTE: This topic describes system log messages for Junos OS processes and libraries and not 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 OS Services Interfaces Configuration Guide*.

Related Documentation

- Junos OS System Log Configuration Statements on page 140
- Junos OS Minimum System Logging Configuration on page 141

Junos OS System Log Configuration Statements

To configure the router 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;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string
    match "regular-expression";
    source-address source-address;
    port port number;
  }
  source-address source-address;
  time-format (year | millisecond | year millisecond);
  user (username | *) {
    facility severity;
    match "regular-expression";
  }
}
```

Related Documentation

- Junos OS System Log Configuration Overview on page 139

Junos OS Minimum and Default System Logging Configuration

For information about the minimum and default system log settings on routers that run the Junos OS, see the following topics:

- Junos OS Minimum System Logging Configuration on page 141
- Junos OS Default System Log Settings on page 141
- Junos OS Platform-Specific Default System Log Messages on page 143

Junos OS 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 13 on page 141. For more information about the configuration statements, see “Single-Chassis System Logging Configuration Overview” on page 144.

Table 13: Minimum Configuration Statements for System Logging

Destination	Minimum Configuration Statements

File	[edit system syslog]
	file *filename* {
	  facility severity;
	}

Terminal session of one, several, or all users	[edit system syslog]
	user (*username* | *) {
	  facility severity;
	}

Router or switch console	[edit system syslog]
	console {
	  facility severity;
	}

Remote machine or the other Routing Engine on the router or switch	[edit system syslog]
	host (*hostname* | other-routing-engine) {
	  facility severity;
	}

Related Documentation

- Junos OS System Log Configuration Overview on page 139
- Overview of Junos OS System Log Messages
- Overview of Single-Chassis System Logging Configuration

Junos OS Default System Log Settings

Table 14 on page 142 summarizes the default system log settings that apply to all routers that run the Junos OS, and specifies which statement to include in the configuration to override the default value.

Table 14: Default System Logging Settings

Setting	Default	Overriding Statement	Instructions

Alternative facility for message forwarded to a remote machine	For **change-log**: **local6**
	
	For **conflict-log**: **local5**
	
	For **dfc**: **local1**
	
	For **firewall**: **local3**
	
	For **interactive-commands**: **local7**
	
	For **pfe**: **local4**
		[edit system syslog]
		host *hostname* {
		  facility-override *facility*;
		}
			"Changing the Alternative Facility Name for Remote System Log Messages" on page 151

Format of messages logged to a file	Standard Junos format, based on UNIX format	[edit system syslog]
		file *filename* {
		  structured-data;
		}
			"Logging Messages in Structured-Data Format" on page 148

Maximum number of files in the archived set	10	[edit system syslog]
		archive {
		  files *number*;
		}
		file *filename* {
		  archive {
		    files *number*;
		  }
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 156

Maximum size of the log file	J Series: 128 kilobytes (KB)
	
	M Series, MX Series, and T Series: 1 megabyte (MB)
	
	TX Matrix: 10 MB
		[edit system syslog]
		archive {
		  size *size*;
		}
		file *filename* {
		  archive {
		    size *size*;
		  }
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 156

Timestamp format	Month, date, hour, minute, second For example: **Aug 21 12:36:30**	[edit system syslog] time-format *format*;	"Including the Year or Millisecond in Timestamps" on page 161

Users who can read log files	**root** user and users with the Junos **maintenance** permission	[edit system syslog]
		archive {
		  world-readable;
		}
		file *filename* {
		  archive {
		    world-readable;
		  }
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 156

- Junos OS System Log Configuration Overview on page 139
- Junos OS Platform-Specific Default System Log Messages on page 143

Junos OS Platform-Specific Default System Log Messages

The following messages are generated by default on specific routers. To view either type of message, you must configure at least one destination for messages as described in "Junos OS Minimum System Logging Configuration" on page 141.

- On J Series routers, a message is logged when a process running in the kernel consumes 500 or more consecutive milliseconds of CPU time.
- To log the kernel process message on an M Series, MX Series, or T Series router, include the **kernel info** statement at the appropriate hierarchy level:

```
[edit system syslog]
(console | file filename | host destination | user username) {
  kernel info;
}
```

- On a routing matrix composed of a TX Matrix router and T640 routers, the master Routing Engine on each T640 router forwards to the master Routing Engine on the TX Matrix router, all messages with a severity of **info** and higher. This is equivalent to the following configuration statement included on the TX Matrix router:

```
[edit system syslog]
host scc-master {
  any info;
}
```

- Likewise, on a routing matrix composed of a TX Matrix Plus router and T1600 routers, the master Routing Engine on each T1600 router forwards to the master Routing Engine on the TX Matrix Plus router all messages with a severity of **info** and higher. This is equivalent to the following configuration statement included on the TX Matrix Plus router:

```
[edit system syslog]
host sfc0-master {
  any info;
}
```

Related Documentation

- Junos OS System Log Configuration Overview on page 139
- Junos OS Default System Log Settings on page 141

Single-Chassis System Logging Configuration

This section includes the following topics:

Single-Chassis System Logging Configuration Overview

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 OS.

System logging configuration for the Junos-FIPS software and for Juniper Networks routers in a Common Criteria environment is the same as for the Junos OS. For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

For information about configuring system logging for a routing matrix composed of a TX Matrix router and T640 routers, see "Configuring System Logging for a TX Matrix Router" on page 167.

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 router functions. You always specify the facility and severity of the messages to include in the log. For more information, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 145.

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 System Log Messages to a Log File" on page 147.
- To the terminal session of one or more specific users (or all users) when they are logged in to the router, by including the **user** statement. See "Directing System Log Messages to a User Terminal" on page 149.
- To the router console, by including the **console** statement. See "Directing System Log Messages to the Console" on page 149.
- To a remote machine that is running the **syslogd** utility or to the other Routing Engine on the router, by including the **host** statement. See "Directing System Log Messages to a Remote Machine or the Other Routing Engine" on page 150.

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 OS System Log Messages Reference*. You can alter the content and format of logged messages in the following ways:

- 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 148.
- 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 (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 158.
- 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 161.
- 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 OS or messages generated on particular routers. For more information, see "Directing System Log Messages to a Remote Machine or the Other Routing Engine" on page 150.
- 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 162.

Related Documentation

- Examples: Configuring System Logging on page 165
- Specifying the Facility and Severity of Messages to Include in the Log on page 145
- Junos OS System Logging Facilities and Message Severity Levels on page 146
- Directing System Log Messages to a Log File on page 147
- Directing System Log Messages to a User Terminal on page 149
- Directing System Log Messages to the Console on page 149
- Directing System Log Messages to a Remote Machine or the Other Routing Engine on page 150

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 router 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;
}
```

Related Documentation

- Junos OS System Logging Facilities and Message Severity Levels on page 146
- Single-Chassis System Logging Configuration Overview on page 144
- Examples: Configuring System Logging on page 165
- Overview of Single-Chassis System Logging Configuration

Junos OS System Logging Facilities and Message Severity Levels

Table 15 on page 146 lists the Junos system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 15: Junos OS 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 OS configuration
conflict-log	Specified configuration is invalid on the router 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 OS command-line interface (CLI) prompt or by a client application such as a Junos XML protocol or NETCONF XML client
kernel	Actions performed or errors encountered by the Junos OS kernel
pfe	Actions performed or errors encountered by the Packet Forwarding Engine

Table 15: Junos OS System Logging Facilities *(continued)*

Facility	Type of Event or Error
user	Actions performed or errors encountered by user-space processes

Table 16 on page 147 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 the System Logging of a Facility" on page 164.

Table 16: 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 router 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 at 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

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Single-Chassis System Logging Configuration
- Examples: Configuring System Logging on page 165

Directing System Log 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;
```

```
    archive <archive-sites (ftp-url <password password>)> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
      brief;
    }
  }
```

For the list of facilities and severity levels, see “Specifying the Facility and Severity of Messages to Include in the Log” on page 145.

To prevent log files from growing too large, the Junos OS 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, either for all log files or for a certain log file. For more information, see “Specifying Log File Size, Number, and Archiving Properties” on page 156.

For information about the following statements, see the indicated sections:

- **explicit-priority**—See “Including Priority Information in System Log Messages” on page 158
- **match**—See “Using Regular Expressions to Refine the Set of Logged Messages” on page 162
- **structured-data**—See “Logging Messages in Structured-Data Format” on page 148

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Junos OS System Log Messages
- Logging Messages in Structured-Data Format
- Examples: Configuring System Logging on page 165
- Examples: Configuring System Logging

Logging Messages in Structured-Data Format

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, *The syslog Protocol*, which is at http://tools.ietf.org/html/draft-ietf-syslog-protocol-23. 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 OS 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.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Examples: Configuring System Logging on page 165

Directing System Log 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 OS 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 145. For information about the **match** statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 162.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Single-Chassis System Logging Configuration
- Examples: Configuring System Logging on page 165
- Examples: Configuring System Logging

Directing System Log 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 145.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Single-Chassis System Logging Configuration
- Examples: Configuring System Logging on page 165
- Examples: Configuring System Logging

System Logging on a Remote Machine or the Other Routing Engine

This section includes the following topics:

Directing System Log 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 router, 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 router. 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 router 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 145.

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 158.

For information about the **match** statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 162.

When directing messages to remote machines, you can include the **source-address** statement to specify the IP address of the router 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.

Related Documentation

- Single-Chassis System Logging Configuration Overview

Specifying an Alternative Source Address for System Log Messages

To specify the router 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 router 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.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Examples: Assigning an Alternative Facility on page 155

Changing the Alternative Facility Name for Remote System Log Messages

Some facilities assigned to messages logged on the local router or switch have the Junos OS–specific names (see Table 15 on page 146). In the recommended configuration, a remote machine designated at the **[edit system syslog host *hostname*]** hierarchy level is not a Juniper Networks router or switch, so its **syslogd** utility cannot interpret the Junos OS–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 OS–specific facility name.

Table 17 on page 153 lists the default alternative facility name next to the Junos OS–specific facility name it is used for.

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 router or switch or the remote machine itself). For example, the following statements in the configuration of the router 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 18 on page 154 lists the facilities that you can specify in the **facility-override** statement.

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 OS system logging utility can interpret the Junos OS–specific names.

The following example shows how to log all messages generated on the local router 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;
```

```
}
```

The following example shows how to configure routers located in California and routers 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 routers to aggregate messages in the **local0** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
  change-log info;
  facility-override local0;
}
```

- Configure New York routers 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**.

Related Documentation

- Table 17 on page 153
- Junos OS System Log Alternate Facilities for Remote Logging on page 154
- Examples: Assigning an Alternative Facility on page 155
- Examples: Assigning an Alternative Facility

System Log Default Facilities for Messages Directed to a Remote Destination

Table 17 on page 153 lists the default alternative facility name next to the Junos OS–specific facility name it is used for. For facilities that are not listed, the default alternative name is the same as the local facility name.

Table 17: Default Facilities for Messages Directed to a Remote Destination

Junos OS–specific Local Facility	Default Facility When Directed to Remote Destination
change-log	local6
conflict-log	local5
dfc	local1
firewall	local3
interactive-commands	local7

Table 17: Default Facilities for Messages Directed to a Remote Destination *(continued)*

Junos OS–specific Local Facility	Default Facility When Directed to Remote Destination
pfe	**local4**

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Single-Chassis System Logging Configuration

Junos OS System Log Alternate Facilities for Remote Logging

Table 18 on page 154 lists the facilities that you can specify in the **facility-override** statement.

Table 18: 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 OS 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 OS system logging utility can interpret the Junos OS–specific names.

Related Documentation

- Examples: Assigning an Alternative Facility on page 155
- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Single-Chassis System Logging Configuration

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**.

Related Documentation

- Junos OS System Log Alternate Facilities for Remote Logging on page 154

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 OS 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.

The following example shows how to 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'
```

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Specifying Log File Size, Number, and Archiving Properties on page 156
- Overview of Single-Chassis System Logging Configuration

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 megabyte (MB) for M Series, MX Series, and T Series routers
- 10 MB for TX Matrix or TX Matrix Plus routers
- 1 MB for the QFX Series

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 OS **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:

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:

archive <archive-sites (*ftp-url* <password *password*>)> <files *number*> <size *size*> <start-time "*YYYY-MM-DD.hh:mm*"> <transfer-interval *minutes*> <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 or switch 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 filename. For information about how to specify valid FTP URLs, see "Format for Specifying Filenames and URLs in Junos OS CLI Commands" on page 46.

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 "*YYYY-MM-DD.hh:mm*" defines the date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

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.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Examples: Configuring System Logging on page 165
- Overview of Single-Chassis System Logging Configuration

Including Priority Information in System Log Messages

The facility and severity level of a message are together referred to as its *priority*. By default, messages logged in the standard Junos OS 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. 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 148. For information about the contents of a structured-data message, see the *Junos OS 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;

NOTE: The **other-routing-engine** option does not apply to the QFX Series.

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 OS 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 System Log Messages" on page 151.

When the **explicit-priority** statement is included, the Junos OS 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 OS system log messages; for more information, see the *Junos OS System Log Messages Reference*.)

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 OS System Log Messages Reference*.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Single-Chassis System Logging Configuration
- Examples: Configuring System Logging on page 165

System Log Facility Codes and Numerical Codes Reported in Priority Information

Table 19 on page 159 lists the facility codes that can appear in system log messages and maps them to facility names.

NOTE: If the second column in Table 19 on page 159 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 OS might use the facilities in Table 19 on page 159—and others that are not listed—when reporting on internal operations.

Table 19: 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 router 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

Table 19: Facility Codes Reported in Priority Information *(continued)*

Code	Junos Facility Name	Type of Event or Error
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 OS CLI prompt or invoked by a client application such as a Junos XML protocol 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 20 on page 160 lists the numerical severity codes that can appear in system log messages and maps them to severity levels.

Table 20: Numerical Codes for Severity Levels Reported in Priority Information

Numerical Code	Severity Level	Description
0	emergency	System panic or other condition that causes the router 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

Table 20: Numerical Codes for Severity Levels Reported in Priority Information *(continued)*

Numerical Code	Severity Level	Description
7	**debug**	Software debugging messages (these appear only if a technical support representative has instructed you to configure this severity level)

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Examples: Configuring System Logging on page 165

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 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 148. For information about the contents of a structured-data message, see the *Junos OS System Log Messages Reference*.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Examples: Configuring System Logging on page 165

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 a specific user session or for all user sessions on a terminal)
- **[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 21 on page 162 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 21: 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 appears 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 OS–specific.

Table 21: Regular Expression Operators for the match Statement *(continued)*

Operator	Matches
ˆ (caret)	Start of a line, when the caret appears outside square brackets. 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)	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.

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 a severity of **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.*”;
}
```

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Single-Chassis System Logging Configuration
- Examples: Configuring System Logging on page 165
- Examples: Configuring System Logging

Junos System Log Regular Expression Operators for the match Statement

Table 22: 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 OS–specific.
^ (caret)	The start of a line, when the caret appears outside square brackets. 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.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Examples: Configuring System Logging on page 165

Disabling the System 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;
  }
```

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144
- Overview of Single-Chassis System Logging Configuration

Examples: Configuring System Logging

The following example shows how to configure the logging of messages about all commands entered by users at the CLI prompt or invoked by client applications such as Junos XML protocol 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;
  }
}
```

The following example shows how to configure the logging of all changes in the state of alarms to the file /var/log/alarms:

```
[edit system]
syslog {
  file alarms {
    kernel warning;
  }
}
```

The following example shows how to 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;
    }
  }
```

The following example shows how to configure the handling of messages generated when users issue Junos OS 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;
  }
}
```

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 144

System Logging Configuration for a TX Matrix Router

This section explains how to configure system logging for a TX Matrix router and the T640 routers in a routing matrix. It assumes you are familiar with system logging for single-chassis systems, as described in "Single-Chassis System Logging Configuration Overview" on page 144. For more information about a TX Matrix router and routing matrix, see the *TX Matrix Router Hardware Guide*.

Configuring System Logging for a TX Matrix Router

To configure system logging for all routers in a routing matrix composed of a TX Matrix router and T640 routers, include the **syslog** statement at the **[edit system]** hierarchy level on the TX Matrix router. The **syslog** statement applies to every router in the routing matrix.

```
[edit system]
syslog {
  archive <files number> <size size <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    port port number;
  }
```



```
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    (username | *) {
      facility severity;
      match "regular-expression";
    }
  }
```

When included in the configuration on the TX Matrix router, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every router 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 156.
- **console**—Directs the specified messages to the console of each platform in the routing matrix. See “Directing System Log Messages to the Console” on page 149.
- **file**—Directs the specified messages to a file of the same name on each platform in the routing matrix. See “Directing System Log Messages to a Log File” on page 147.
- **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 162.

  The separate **match** statement at the **[edit system syslog host scc-master]** hierarchy level applies to messages forwarded from the T640 routers to the TX Matrix router. See “Configuring Optional Features for Forwarded Messages on a TX Matrix Router” on page 172.
- **port**—Specifies the port number of the remote syslog server.
- **source-address**—Sets the IP address of the router 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. On a routing matrix composed of a TX Matrix router and T640 routers, the address is not reported by the T640 routers in messages directed to the other Routing Engine on each router or to the TX Matrix router. See “Specifying an Alternative Source Address for System Log Messages” on page 151.
- **structured-data**—Writes messages to a file in structured-data format. See “Logging Messages in Structured-Data Format” on page 148.
- **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 161.
- **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 System Log Messages to a User Terminal” on page 149.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system.

Related Documentation

- Configuring Message Forwarding to the TX Matrix Router on page 169
- Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router on page 170
- Configuring Optional Features for Forwarded Messages on a TX Matrix Router on page 172
- Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router on page 173
- Configuring System Logging Differently on Each T640 Router in a Routing Matrix on page 174

Configuring Message Forwarding to the TX Matrix Router

By default, the master Routing Engine on each T640 router forwards to the master Routing Engine on the TX Matrix router 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 router:

```
[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 routers in the routing matrix.

To capture the messages forwarded by the T640 routers (as well as messages generated on the TX Matrix router itself), you must also configure system logging on the TX Matrix router. Direct the messages to one or more destinations by including the appropriate statements at the **[edit system syslog]** hierarchy level on the TX Matrix router:

- To a file, as described in “Directing System Log Messages to a Log File” on page 147.
- To the terminal session of one or more specific users (or all users), as described in “Directing System Log Messages to a User Terminal” on page 149.
- To the console, as described in “Directing System Log Messages to the Console” on page 149.
- 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 Based on the TX Matrix Router” on page 173.

As previously noted, the configuration statements included on the TX Matrix router also configure the same destinations on each T640 router in the routing matrix.

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.)

Related Documentation

- Configuring System Logging for a TX Matrix Router on page 167

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router

This topic describes the impact of different local and forwarded severity levels configured for system log messages on a TX Matrix router:

Messages Logged When the 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 router contains all messages from the logs on the T640 routers. For example, you can specify severity **info** for the */var/log/messages* file, which is the default severity level for messages forwarded by T640 routers:

```
[edit system syslog]
file messages {
  any info;
}
```

Table 23 on page 170 specifies which messages are included in the logs on the T640 routers and the TX Matrix router.

Table 23: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**info**
TX Matrix router	Local	**info**
	Forwarded from T640 routers	**info**

Messages Logged When the Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix router 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, on a TX Matrix router, 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 24 on page 171 specifies which messages in a routing matrix are included in the logs on the T640 routers and the TX Matrix router. The T640 routers forward only those messages with severity **critical** and higher, so the log on the TX Matrix router does not include the messages with severity **error**, **warning**, or **notice** that the T640 routers log locally.

Table 24: Example: Local Severity Is notice, Forwarded Severity Is critical

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**notice**
TX Matrix router	Local	**notice**
	Forwarded from T640 routers	**critical**

Messages Logged When the Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix router 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 25 on page 172 specifies which messages are included in the logs on the T640 routers and the TX Matrix router. Although the T640 routers forward messages with severity **notice** and higher, the TX Matrix router discards any of those messages with severity lower than **critical** (does not log forwarded messages with severity **error**, **warning**, or **notice**). None of the logs include messages with severity **error** or lower.

Table 25: Example: Local Severity Is critical, Forwarded Severity Is notice

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**critical**
TX Matrix router	Local	**critical**
	Forwarded from T640 routers	**critical**

Related Documentation

- Configuring System Logging for a TX Matrix Router on page 167

Configuring Optional Features for Forwarded Messages on a TX Matrix Router

To configure additional optional features when specifying how the T640 routers forward messages to the TX Matrix router, 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";
}
```

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 router, because it runs the Junos system logging utility and can interpret the Junos OS–specific facilities. For more information about alternative facilities, see “Changing the Alternative Facility Name for Remote System Log Messages” on page 151.

- Including Priority Information in Forwarded Messages on page 172
- Adding a Text String to Forwarded Messages on page 173
- Using Regular Expressions to Refine the Set of Forwarded Messages on page 173

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 router include priority information. For the information to appear in a log file on the TX Matrix router, you must also include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level for the file on the TX Matrix router. 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 routers 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 Based on the TX Matrix Router” on page 173.

In the following example, the /var/log/messages file on all routers includes priority information for messages with severity **notice** and higher from all facilities. The log on the TX Matrix router also includes messages with those characteristics forwarded from the T640 routers.

```
[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 router. For more information, see “Adding a Text String to System Log Messages” on page 155.

Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the **match** statement at the **[edit system syslog host scc-master]** hierarchy level, the regular expression that you specify controls which messages from the T640 routers are forwarded to the TX Matrix router. The regular expression is not applied to messages from the T640 router that are directed to destinations other than the TX Matrix router. For more information about regular expression matching, see “Using Regular Expressions to Refine the Set of Logged Messages” on page 162.

Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router

You can configure a routing matrix composed of a TX Matrix router and T640 routers to direct system logging messages to a remote machine or the other Routing Engine on each router, just as on a single-chassis system. Include the **host** statement at the **[edit system syslog]** hierarchy level on the TX Matrix router:

```
[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 router 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 System Log Messages to a Remote Machine or the Other Routing Engine" on page 150.

For the TX Matrix router to include priority information when it directs messages that originated on a T640 router 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 routers to the TX Matrix router. 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 router 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 router.

Because the configuration on the TX Matrix router applies to the T640 routers, any T640 router that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the T640 routers are configured to forward messages to the TX Matrix router (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T640 router and the other from the TX Matrix router. 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 to the TX Matrix Router" on page 169.
- If the **source-address** statement is configured at the **[edit system syslog]** hierarchy level, all routers 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 router.
- If the **log-prefix** statement is included, the messages from all routers in the routing matrix include the same text string. You cannot use the string to distinguish between the routers in the routing matrix.

Related Documentation

- Configuring System Logging for a TX Matrix Router on page 167

Configuring System Logging Differently on Each T640 Router in a Routing Matrix

We recommend that all routers in a routing matrix composed of a TX Matrix router and T640 routers use the same configuration, which implies that you include system logging configuration statements on the TX Matrix router only. In rare circumstances, however, you might choose to log different messages on different routers. For example, if one router 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 router.

To configure routers separately, include configuration statements in the appropriate groups at the **[edit groups]** hierarchy level on the TX Matrix router:

- To configure settings that apply to the TX Matrix router but not the T640 routers, include them in the **re0** and **re1** configuration groups.
- To configure settings that apply to particular T640 routers, 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 router.

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 router. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T640 routers also. (We further recommend that you do not issue CLI configuration-mode commands on the T640 routers at any time.)

For more information about the configuration groups for a routing matrix, see the chapter about configuration groups in the *Junos OS CLI User Guide*.

The following example shows how to configure the /var/log/messages files on three routers to include different sets of messages:

- On the TX Matrix router, local messages with severity **info** and higher from all facilities. The file does not include messages from the T640 routers, because the **host scc-master** statement disables message forwarding.
- On the T640 router designated **LCC0**, messages from the **authorization** facility with severity **info** and higher.
- On the T640 router 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 ...
}
```

Related Documentation

- Configuring System Logging for a TX Matrix Router on page 167

System Logging Configuration for a TX Matrix Plus Router

This section explains how to configure system logging for a TX Matrix Plus router and the T1600 routers in a routing matrix. It assumes you are familiar with system logging for single-chassis systems, as described in "Single-Chassis System Logging Configuration Overview" on page 144. For more information about a TX Matrix Plus router and routing matrix, see the *TX Matrix Router Hardware Guide*.

Configuring System Logging for a TX Matrix Plus Router

To configure system logging for all routers in a routing matrix composed of a TX Matrix Plus router and T1600 routers, include the **syslog** statement at the **[edit system]** hierarchy level on the TX Matrix Plus router. The **syslog** statement applies to every router in the routing matrix.

```
[edit system]
syslog {
   archive <files number> <size size <world-readable | no-world-readable>;
   console {
      facility severity;
```



```
    }
    file filename {
      facility severity;
      archive <archive-sites {ftp-url <password password>}> <files number> <size size>
        <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
        no-world-readable>;
      explicit-priority;
      match "regular-expression";
      structured-data {
        brief;
      }
    }
    host (hostname | other-routing-engine | sfc0-master) {
      facility severity;
      explicit-priority;
      facility-override facility;
      log-prefix string;
      match "regular-expression";
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    (username | *) {
      facility severity;
      match "regular-expression";
    }
  }
```

When included in the configuration on the TX Matrix Plus router, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every router in the routing matrix composed of the TX Matrix Plus router and T1600 routers:

- **archive**—Sets the size and number of log files on each router in the routing matrix. See “Specifying Log File Size, Number, and Archiving Properties” on page 156.
- **console**—Directs the specified messages to the console of each router in the routing matrix. See “Directing System Log Messages to the Console” on page 149.
- **file**—Directs the specified messages to a file of the same name on each router in the routing matrix. See “Directing System Log Messages to a Log File” on page 147.
- **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 162.

  The separate **match** statement at the **[edit system syslog host sfc0-master]** hierarchy level applies to messages forwarded from the T1600 routers to the TX Matrix Plus router. See “Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router” on page 181.
- **source-address**—Sets the IP address of the router as the message source in system log messages when the messages are directed to the remote machines specified in all **host** *hostname* statements at the **[edit system syslog]** hierarchy level, for each router in the routing matrix. On a routing matrix composed of a TX Matrix Plus router and T1600 routers, the address is not reported by the T1600 routers in messages directed

to the other Routing Engine on each router or to the TX Matrix Plus router. See "Specifying an Alternative Source Address for System Log Messages" on page 151.

- **structured-data**—Writes messages to a file in structured-data format. See "Logging Messages in Structured-Data Format" on page 148.
- **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 161.
- **user**—Directs the specified messages to the terminal session of one or more specified users on each router in the routing matrix that they are logged in to. See "Directing System Log Messages to a User Terminal" on page 149.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system.

Related Documentation

- Configuring Message Forwarding to the TX Matrix Plus Router on page 178
- Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router on page 179
- Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router on page 181
- Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router on page 183
- Configuring System Logging Differently on Each T1600 Router in a Routing Matrix on page 184

Configuring Message Forwarding to the TX Matrix Plus Router

By default, the master Routing Engine on each T1600 router forwards to the master Routing Engine on the TX Matrix Plus router all messages from all facilities with severity level of **info** and higher. To change the facility, the severity level, or both, include the **host sfc0-master** statement at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router:

```
[edit system syslog]
host sfc0-master {
  facility severity;
}
```

To disable message forwarding, set the facility to **any** and the severity level to **none**:

```
[edit system syslog]
host sfc0-master {
  any none;
}
```

In either case, the setting applies to all T1600 routers in the routing matrix.

To capture the messages forwarded by the T1600 routers (as well as messages generated on the TX Matrix Plus router itself), you must also configure system logging on the TX Matrix Plus router. Direct the messages to one or more destinations by including the appropriate statements at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router:

- To a file, as described in "Directing System Log Messages to a Log File" on page 147.
- To the terminal session of one or more specific users (or all users), as described in "Directing System Log Messages to a User Terminal" on page 149.
- To the console, as described in "Directing System Log Messages to the Console" on page 149.
- 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 Based on a TX Matrix Plus Router" on page 183.

As previously noted, the configuration statements included on the TX Matrix Plus router also configure the same destinations on each T1600 router.

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 sfc0-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.)

Related Documentation

- Configuring System Logging for a TX Matrix Plus Router on page 176

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router

This topic describes the impact of different local and forwarded severity levels configured for the system log messages on a TX Matrix Plus router:

Messages Logged When the 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 Plus router contains all messages from the logs on the T1600 routers in the routing matrix. For example, you can specify severity **info** for the */var/log/messages* file, which is the default severity level for messages forwarded by T1600 routers:

```
[edit system syslog]
file messages {
  any info;
}
```

Table 26 on page 180 specifies which messages in a routing matrix based on a TX Matrix Plus router are included in the logs on the T1600 routers and the TX Matrix Plus router:

Table 26: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	**info**
TX Matrix Plus router	Local	**info**
	Forwarded from T1600 routers	**info**

Messages Logged When the Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix Plus router 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, on a TX Matrix Plus router, 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 sfc0-master {
   any critical;
}
```

Table 27 on page 180 specifies which messages in a routing matrix are included in the logs on the T1600 routers and the TX Matrix Plus router. The T1600 routers forward only those messages with severity **critical** and higher, so the log on the TX Matrix Plus router does not include the messages with severity **error**, **warning**, or **notice** that the T1600 routers log locally.

Table 27: Example: Local Severity Is notice, Forwarded Severity Is critical

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	**notice**
TX Matrix Plus router	Local	**notice**
	Forwarded from T1600 routers	**critical**

Messages Logged When the Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix Plus router 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 sfc0-master {
  any notice;
}
```

Table 28 on page 181 specifies which messages are included in the logs on the T1600 routers and the TX Matrix Plus router. Although the T1600 routers forward messages with severity **notice** and higher, the TX Matrix Plus router discards any of those messages with severity lower than **critical** (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
T1600 router	Local	**critical**
TX Matrix Plus router	Local	**critical**
	Forwarded from T1600 routers	**critical**

Related Documentation

- Configuring System Logging for a TX Matrix Plus Router on page 176

Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router

To configure additional optional features when specifying how the T1600 routers forward messages to the TX Matrix Plus router, include statements at the **[edit system syslog host sfc0-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 sfc0-master {
  facility severity;
  explicit-priority;
  log-prefix string;
  match "regular-expression;
}
```

You can also include the **facility-override** statement at the **[edit system syslog host sfc0-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 Plus router, because it runs the Junos system logging utility and can interpret the Junos OS–specific facilities.

For more information about alternative facilities, see “Changing the Alternative Facility Name for Remote System Log Messages” on page 151.

Including Priority Information in Forwarded Messages

When you include the **explicit-priority** statement at the **[edit system syslog host sfc0-master]** hierarchy level, messages forwarded to the TX Matrix Plus router include priority information. For the information to appear in a log file on the TX Matrix Plus router, you must also include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level for the file on the TX Matrix Plus router. 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 routers 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 Based on a TX Matrix Plus Router” on page 183.

In the following example, the */var/log/messages* file on all routers includes priority information for messages with severity **notice** and higher from all facilities. The log on the TX Matrix Plus router also includes messages with those characteristics forwarded from the T1600 routers.

```
[edit system syslog]
host sfc0-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 sfc0-master]** hierarchy level, the string that you define appears in every message forwarded to the TX Matrix Plus router. For more information, see “Adding a Text String to System Log Messages” on page 155.

Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the **match** statement at the **[edit system syslog host sfc0-master]** hierarchy level, the regular expression that you specify controls which messages from the T1600 routers are forwarded to the TX Matrix Plus router. The regular expression is not applied to messages from the T1600 routers that are directed to destinations other than the TX Matrix Plus router. For more information about regular expression matching, see “Using Regular Expressions to Refine the Set of Logged Messages” on page 162.

Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router

You can configure a routing matrix composed of a TX Matrix Plus router and T1600 routers to direct system logging messages to a remote machine or the other Routing Engine on each routing router, just as on a single-chassis system. Include the **host** statement at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router:

```
[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 Plus router 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 System Log Messages to a Remote Machine or the Other Routing Engine” on page 150.

For the TX Matrix Plus router to include priority information when it directs messages that originated on a T1600 router to the remote destination, you must also include the **explicit-priority** statement at the **[edit system syslog host sfc0-master]** hierarchy level.

The **other-routing-engine** statement does not interact with message forwarding from the T1600 routers to the TX Matrix Plus router. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (**re0**), the **re0** Routing Engine on each T1600 router sends messages to the **re1** Routing Engine on its router only. It does not also send messages directly to the **re1** Routing Engine on the TX Matrix Plus router.

Because the configuration on the TX Matrix Plus router applies to the T1600 routers, any T1600 router that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the T1600 routers are configured to forward messages to the TX Matrix Plus router (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T1600 router and the other from the TX Matrix Plus router. 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 to the TX Matrix Plus Router” on page 178.
- If the **source-address** statement is configured at the **[edit system syslog]** hierarchy level, all routers 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 router.
- If the **log-prefix** statement is included, the messages from all routers in the routing matrix include the same text string. You cannot use the string to distinguish between the routers in the routing matrix.

Related Documentation

- Configuring System Logging for a TX Matrix Plus Router on page 176

Configuring System Logging Differently on Each T1600 Router in a Routing Matrix

We recommend that all routers in a routing matrix composed of a TX Matrix Plus router and T1600 routers use the same configuration, which implies that you include system logging configuration statements on the TX Matrix Plus router only. In rare circumstances, however, you might choose to log different messages on different routers. For example, if one router 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 router.

To configure routers separately, include configuration statements in the appropriate groups at the **[edit groups]** hierarchy level on the TX Matrix Plus router:

- To configure settings that apply to the TX Matrix Plus router but not the T1600 routers, include them in the **re0** and **re1** configuration groups.
- To configure settings that apply to particular T1600 routers, 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 router.

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 Plus router. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T1600 routers also. (We further recommend that you do not issue CLI configuration-mode commands on the T1600 routers at any time.)

For more information about the configuration groups for a routing matrix, see the chapter about configuration groups in the *Junos OS CLI User Guide*.

The following example shows how to configure the /var/log/messages files on three routers to include different sets of messages:

- On the TX Matrix Plus router, local messages with severity **info** and higher from all facilities. The file does not include messages from the T1600 routers, because the **host sfc0-master** statement disables message forwarding.
- On the T1600 router designated **LCC0**, messages from the **authorization** facility with severity **info** and higher.
- On the T1600 router designated **LCC1**, messages with severity **notice** from all facilities.

```
[edit groups]
re0 {
  system {
    syslog {
      file messages {
        any info;
      }
      host sfc0-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 ...
}
```

Related Documentation

- Configuring System Logging for a TX Matrix Plus Router on page 176

CHAPTER 10

Configuring System Services

This chapter includes the following topics:

System Services Overview

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, Junos XML protocol client applications can use Secure Sockets Layer (SSL) or the Junos XML protocol-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.**

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189
- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190
- DHCP Access Service Overview on page 192
- Configuring the Router as an Extended DHCP Local Server on page 210
- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 212

Configuring clear-text or SSL Service for Junos XML Protocol Client Applications

A Junos XML protocol client application can use one of four protocols to connect to the Junos XML protocol server on a router: clear-text (a Junos XML protocol-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 Junos XML protocol-specific statements in the router configuration.

For more information, see the following topics:

Configuring clear-text Service for Junos XML Protocol Client Applications

To configure the router to accept clear-text connections from Junos XML protocol 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 Junos XML protocol 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 per protocol (IPv4 and IPv6) (a value from **1** through **250**). The default is **75**. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of **10** allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions.
- **rate-limit *limit***—Maximum number of connection attempts accepted per minute per protocol (IPv4 and IPv6). The range is a value from **1** through **250**. The default is **150**. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of **10** allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

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 Junos XML Protocol Client Applications

To configure the router to accept SSL connections from Junos XML protocol 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.

By default, the Junos XML protocol 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 per protocol (IPV4 and IPv6). The range is a value from **1** through **250**. The default is **75**. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of **10** allows 10 IPv6 SSL sessions and 10 IPv4 SSL sessions.
- **rate-limit** ***limit***—Maximum number of connection attempts accepted per protocol per minute. The range is a value from **1** through **250**. The default is **150**. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of **10** allows 10 IPv6 SSL session connection attempts per minute and 10 IPv4 SSL session connection attempts per minute.

Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches

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. On J Series Services Routers and EX Series switches, a router, switch, 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*.

A J Series router or EX Series switch configured as a DHCP server is compatible with the autoinstallation feature.

To configure a J Series router or EX Series switch 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-name hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
  }
  server-identifier address;
  wins-server {
    address;
  }
}
```

Related Documentation

- DHCP Access Service Overview on page 192
- DHCP Statement Hierarchy and Inheritance on page 195

DHCP Access Service 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.

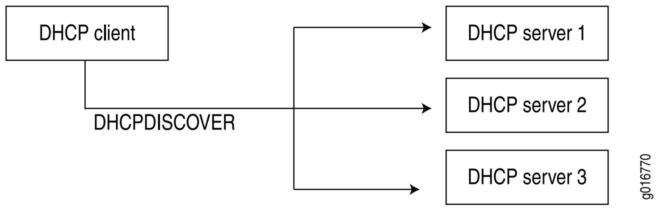
The following topics describe these concepts in detail:

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.

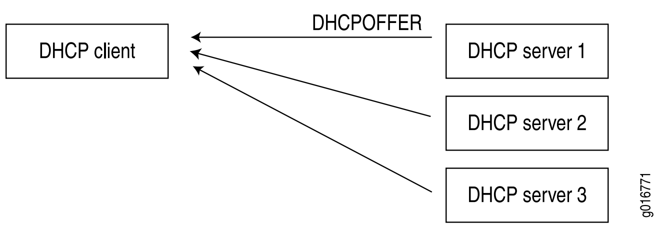
Figure 5: DHCP Discover



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.

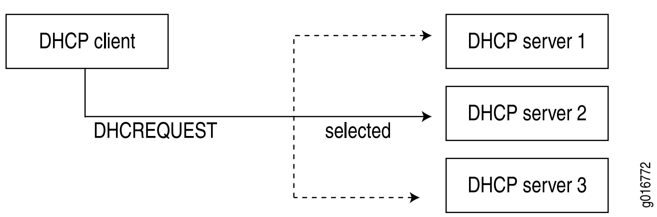
2. Each DHCP server receiving the broadcast sends a **DHCPOFFER** message to the client, offering an IP address for a set period of time, known as the lease period.

Figure 6: DHCP Offer



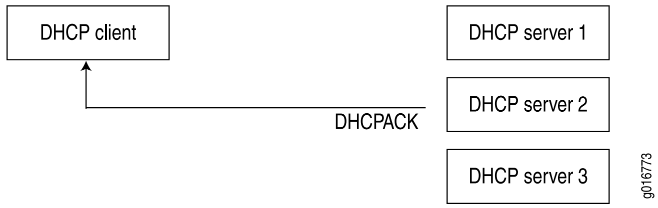
3. The client receives one or more **DHCPOFFER** messages from one or more servers and selects one of the offers received. Normally, a client looks for the longest lease period.
4. The client broadcasts a **DHCPREQUEST** message indicating the client has selected an offered leased IP address and identifies the selected server.

Figure 7: 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 8: DHCP ACK

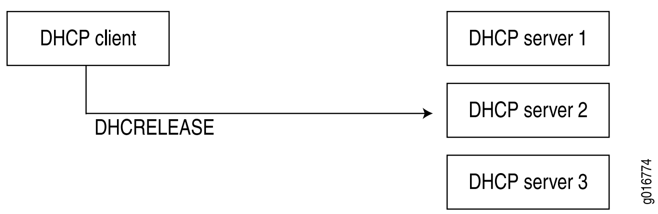


The information offered by the server is configurable.

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 9: 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.

Related Documentation

- DHCP Statement Hierarchy and Inheritance on page 195

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 195.

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 196 (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]** **[edit system services dhcp pool]** **[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.	

Related Documentation

- DHCP Access Service Overview on page 192

Configuring Address Pools for DHCP Dynamic Bindings

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.

Related Documentation

- DHCP Access Service Overview on page 192
- Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address on page 198

Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address

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;
}
```

Related Documentation

- DHCP Access Service Overview on page 192
- Specifying DHCP Lease Times for IP Address Assignments on page 199

Specifying DHCP Lease Times for IP Address Assignments

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;
```

Related Documentation

- DHCP Access Service Overview on page 192
- Configuring a DHCP Boot File and DHCP Boot Server on page 199

Configuring a DHCP Boot File and DHCP Boot Server

When a DHCP 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 | hostname);
```

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 or 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;
}
```

Related Documentation

- DHCP Access Service Overview on page 192
- Configuring a Static IP Address as DHCP Server Identifier on page 201

Configuring the Next DHCP Server to Contact After a Boot Client Establishes Initial Communication

On J Series Services Routers, you can configure the next DHCP server to contact after a DHCP boot client establishes initial communication. You can use this option to specify the IP address of the DHCP server that is used as the “siaddr” in a DHCP protocol packet.

To configure the next server, include the **next-server** ***next-server*** statement at one of the following hierarchy levels:

- **[edit system services dhcp]**
- **[edit system services dhcp pool *pool-id*]**

- **[edit system services dhcp static-binding *mac-address*]**

```
[edit system services dhcp]
next-server next-server;

[edit system services dhcp pool pool-id]
next-server next-server;

[edit system services dhcp static-binging mac-address]
next-server next-server;
```

Related Documentation

- **next-server on page 387**

Configuring a Static IP Address as DHCP Server Identifier

The host running the DHCP server must itself 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 DHCP 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;
}
```

Related Documentation

- DHCP Access Service Overview on page 192

Configuring a Domain Name and Domain Search List for a DHCP Server Host

To configure the name of the domain in which clients 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.

Related Documentation

- DHCP Access Service Overview on page 192

Configuring Routers Available to the DHCP 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 DHCP 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;
}
```

Related Documentation

- DHCP Access Service Overview on page 192

Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server

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-type option-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 **router** statement instead:

```
[edit system services dhcp]
option 3 router 10.7.7.2; # 3: "Default Router" option
router {
```



```
    10.7.7.1;
}
```

Related Documentation

- DHCP Access Service Overview on page 192

Example: Complete DHCP Server Configuration

This topic 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
```

For more information about CLI commands you can use with the DHCP server, see the *Junos OS System Basics and Services Command Reference*.

Configuring Tracing Operations for 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 three trace files. Then the oldest trace file (**dhcpd.2** is overwritten). For more information about how log files are created, see the *Junos OS 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;
}
```

Tasks for configuring DHCP tracing operations are:

1. Configuring the DHCP Processes Log Filename on page 207
2. Configuring the Number and Size of DHCP Processes Log Files on page 207
3. Configuring Access to the DHCP Log File on page 208
4. Configuring a Regular Expression for Refining the Output of DHCP Logged Events on page 208
5. Configuring DHCP Trace Operation Events on page 208

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]
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 three 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 DHCP 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 Refining the Output of DHCP Logged Events

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 DHCP Trace Operation Events

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;
}
```


DHCP Processes Tracing Flags

Table 31 on page 209 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 Router as an 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 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]**

NOTE: The extended DHCP local server is incompatible with the J Series router DHCP server. As a result, the DHCP local server and the DHCP or 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.

Related Documentation

- Example: Configuring the Minimum Extended DHCP Local Server Configuration on page 222
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 222

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.

Extended DHCP Local Server and 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 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.

Methods Used by the Extended DHCP Local Server to Determine 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.

The following sections describe the methods used by the DHCP local server to determine which address-assignment pool to use:

- Matching the Client IP Address to the Address-Assignment Pool on page 213
- Matching Option 82 Information to Named Address Ranges on page 213

Matching the Client IP Address to the 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.

Default Options Provided by the Extended DHCP Server for the DHCP Client

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 to Authenticate DHCP Clients

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 topic 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.

Tasks for configuring External AAA authentication services are:

1. Configuring Authentication Support for an Extended DHCP Application on page 215
2. Grouping Interfaces with Common DHCP Configurations on page 216
3. Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service on page 217
4. Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service on page 217

Configuring Authentication Support for an Extended DHCP Application

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 the DHCP Application Presents to the External AAA Authentication Service

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 "Special Requirements for Junos OS Plain-Text Passwords" on page 72 for information about supported characters in passwords. For example:

```
authentication {
  password myPassworD1234;
}
```

Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service

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 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
```

The following example shows a sample configuration that creates a unique username. The username is shown after the configuration.

```
authentication {
  username-include {
    circuit-type;
    domain-name isp55.com;
    mac-address;
    user-prefix wallybrown;
  }
```

```
}
```

The resulting unique username is:

```
wallybrown.0090.1a01.1234.enet@isp55.com
```

Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client

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 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 three 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;
}
```

The following topics describe the tracing operation configuration statements:

Configuring the Filename of the Extended DHCP Local Server Processes Log

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 Lines 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: Configuring the 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:

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.**

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
  }
}
```

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 the DHCP 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 per protocol (IPv4 and IPv6). The range is a value from **1** through **250**. The default is **75**. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of **10** allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions.

- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute per protocol (IPv4 and IPv6). The range is a value from **1** through **250**. The default is **150**. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of **10** allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

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.

You can also specify user permissions through the Juniper-User-Permissions RADIUS attribute.

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.

Configuring Finger Service for Remote Access to the Router

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 per protocol (IPv4 and IPv6). The range is a value from **1** through **250**. The default is **75**. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of **10** allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (a value from **1** through **250**). The default is **150**. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of **10** allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

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 for Remote Access to the Router or Switch

To configure the router or switch 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 or switch supports a limited number of simultaneous FTP sessions and connection attempts per minute. You can include either or both of the following statements to change the defaults:

- **connection-limit** *limit*—Maximum number of simultaneous connections per protocol (IPV4 and IPv6). The range is a value from **1** through **250**. The default is **75**. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of **10** allows 10 IPv6 FTP sessions and 10 IPv4 FTP sessions.
- **rate-limit** *limit*—Maximum number of connection attempts accepted per minute (a value from **1** through **250**). The default is **150**.When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of **10** allows 10 IPv6 FTP session connection attempts and 10 IPv4 FTP session connection attempts.

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 or switches that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

Configuring SSH Service for Remote Access to the Router or Switch

To configure the router or switch 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 or switch supports a limited number of simultaneous SSH sessions and connection attempts per minute. Include either or both of the following statements to change the defaults:

- **connection-limit** ***limit***—Maximum number of simultaneous connections per protocol (IPV4 and IPv6). The range is a value from **1** through **250**. The default is **75**. When you configure a connection limit, the limit is applicable to the number of SSH sessions per protocol (IPv4 and IPv6). For example, a connection limit of **10** allows 10 IPv6 SSH sessions and 10 IPv4 SSH sessions.
- **rate-limit** ***limit***—Maximum number of connection attempts accepted per minute (a value from **1** through **250**). The default is **150**. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of **10** allows 10 IPv6 SSH session connection attempts per minute and 10 IPv4 SSH session connection attempts per minute.

For information about other configuration settings, see the following topics:

- Configuring the Root Login Through SSH on page 226
- Configuring the SSH Protocol Version on page 227

Configuring the Root Login Through SSH

By default, users are allowed to log in to the router or switch 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 or switch as root through SSH. The default is **allow**.

deny—Disables users from logging in to the router or switch as root through SSH.

deny-password—Allows users to log in to the router or switch as root through SSH when the authentication method (for example, RSA) does not require a password.

Configuring the SSH Protocol Version

By default, both version 1 and version 2 of the SSH protocol are enabled. To configure the router or switch to use only version 1 of 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 or switch to use only version 2 of the SSH protocol, include the **protocol-version** statement and specify **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v2 ];
```

To explicitly configure the router or switch 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 ];
```

For J Series Services Routers, the export license software supports SSH version 1 only.

Configuring Outbound SSH Service

You can configure a router or switch running the Junos OS 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 or switch is behind a firewall). A single **outbound-ssh** configuration statement instructs the router or switch to create a TCP/IP connection with the client management application and to forward the identity of the router or switch. Once the connection is established, the management application initiates the SSH sequence as the client and the router or switch 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 or switch 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 or switch and the client management application is broken, the router or switch 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 or switch 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 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;
         }
      }
```

The following topics describe the tasks for configuring the outbound-SSH service:

Configuring the Device Identifier for Outbound SSH Connections

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of ***device-id***.

To configure the device identifier of the router or switch, 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 Public SSH Host Key to the Outbound SSH Client

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of ***device-id***.

To configure the device identifier of the router or switch, 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
```

During the initialization of an SSH connection, the client authenticates the identity of the router or switch using the public SSH host key of the router or switch. Therefore, before the client can initiate the SSH sequence, it needs the public SSH key of the router or switch. When you configure the **secret** statement, the router or switch passes its public SSH key as part of the outbound SSH connection initiation sequence.

When the **secret** statement is set and the router or switch establishes an outbound SSH connection, the router or switch 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 or switch 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 or switch identified by the **device-id** statement.

Using the **secret** statement to transport the 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 or switch sends its public SSH host key every time it 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 or switch. 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 send the router's or switch's public SSH host key when the router or switch connects to the client, 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 following message is sent by the router or switch 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
```

Configuring Keepalive Messages for Outbound SSH Connections

Once the client application has the router's or switch's public SSH host key, it can then initiate the SSH sequence as if it had created the TCP/IP connection and can authenticate the router or switch using its copy of the router's or switch's public host SSH key as part of that sequence. The router or switch authenticates the client user through the mechanisms supported in the Junos OS (RSA/DSA public string or password authentication).

To enable the router or switch 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** statement specifies how long the router or switch waits to receive data before sending a request for acknowledgment from the application. The default is 15 seconds.

The **retry** statement specifies how many keepalive messages the router sends without receiving a response from the client. When that number is exceeded, the router or switch disconnects from the application, ending the outbound SSH connection. The default is three retries.

Configuring a New Outbound SSH Connection

When disconnected, the router or switch begins to initiate a new outbound SSH connection. To specify how the router or switch 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 or switch to reconnect to the server from which it disconnected.

The **in-order** option configures the router or switch to reconnect to the first configured server. If this server is unavailable, the router or switch 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 the reconnection attempts stop. See "Configuring Keepalive Messages for Outbound SSH Connections" on page 230.

Configuring the Outbound SSH Client to Accept NETCONF as an Available Service

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 address {
    retry number;
    timeout seconds;
    port port-number;
  }
```

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.

The **address *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 or switch can make 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 NETCONF-Over-SSH Connections on a Specified TCP Port

The Junos OS enables you to restrict incoming NETCONF connections to a specified TCP port without configuring a firewall. To configure the TCP port used for NETCONF-over-SSH connections, include the **port** statement at the **[edit system services netconf ssh]** hierarchy level. The configured port accepts only NETCONF-over-SSH sessions. Regular SSH session requests for this port are rejected.

You can either configure the default port **830** for NETCONF connections over SSH, as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*, or configure any port from **1** through **65535**.

NOTE:

- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

Related Documentation

- **port (NETCONF Server) on page 406**

Configuring Telnet Service for Remote Access to a Router or Switch

To configure the router or switch 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 or switch 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 per protocol (IPV4 and IPv6). The range is from **1** through **250**. The default is **75**. When you configure a connection limit, the limit is applicable to the number of telnet sessions per protocol (IPv4 and IPv6). For example, a connection limit of **10** allows 10 IPv6 telnet sessions and 10 IPv4 telnet sessions.
- **rate-limit** ***limit***—Maximum number of connection attempts accepted per minute (from **1** through **250**). The default is **150**. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of **10** allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

You cannot include the **telnet** statement on devices that run the Junos-FIPS software. We recommend that you do not use Telnet in a Common Criteria environment.

CHAPTER 11

Configuring Miscellaneous System Management Features

This chapter includes the following topics:

Configuring the Junos OS to Set Console and Auxiliary Port Properties

Each router or switch has a console port and an auxiliary port for connecting terminals to the router or switch. 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 {
    disable;
    insecure;
    type terminal-type;
  }
  console {
    disable;
    insecure;
    log-out-on-disconnect;
    type terminal-type;
  }
}
```

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 identifier (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.

Related Documentation

- Methods for Configuring Junos OS on page 19
- **console on page 326**
- **ports on page 409**

Configuring the Junos OS to Disable Protocol Redirect Messages on the Router or Switch

By default, the router or switch sends protocol redirect messages. To disable the sending of redirect messages by the router or switch, 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 or switch, 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.

Related Documentation

- Configuring the Junos OS to Ignore ICMP Source Quench Messages on page 256
- Configuring the Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets
- *Junos OS Network Interfaces Configuration Guide*

Configuring the Junos OS to Select a Fixed 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 OS 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 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.

Related Documentation

- Configuring the Junos OS to Disable Protocol Redirect Messages on the Router or Switch on page 235
- **default-address-selection on page 328**

Configuring the Junos OS to Make the Router or Interface Act as a DHCP or BOOTP Relay Agent

To configure a router or interface to act as a bootstrap protocol (DHCP or BOOTP) relay agent, you include statements at the **[edit forwarding-options helpers]** hierarchy level.

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.

NOTE: **You cannot configure a router or interface as a DHCP server and a BOOTP relay agent at the same time.**

Configuring the Junos OS to Disable the Routing Engine 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 or switches in the network.

Related Documentation

- Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 237

Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses

When you issue the **ping** command with the **record-route** option, the Routing Engine displays the path of the ICMP echo request packets and timestamps in the ICMP echo responses by default.

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 or switch and its loopback address.

Related Documentation

- Configuring the Junos OS to Disable the Routing Engine Response to Multicast Ping Packets on page 237

Configuring Password Authentication for 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.

Related Documentation

- Configuring the Junos OS to Set Console and Auxiliary Port Properties on page 234
- Configuring Password Authentication for the Diagnostics Port on page 241

Configuring the Junos OS to Display 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.

You can format the message using the following special characters:

- \n—New line
- \t—Horizontal tab
- \'—Single quotation mark
- \"—Double quotation mark
- \\—Backslash

The following is a sample 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 preceding login message configuration example produces 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 the Junos OS to Display a System Login Announcement” on page 240.

Related Documentation

- Configuring the Junos OS to Display a System Login Announcement on page 240
- Defining Junos OS Login Classes on page 78

Configuring the Junos OS to Display 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 the Junos OS to Display a System Login Message" on page 238.

TIP: You can use the same special characters described in "Configuring the Junos OS to Display a System Login Message" on page 238 to format your system login announcement.

Related Documentation

- Configuring the Junos OS to Display a System Login Message on page 238

Disabling Junos OS 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**.

Related Documentation

- Configuring Failover to Backup Media if a Junos OS Process Fails on page 241
- Configuring Password Authentication for the Diagnostics Port on page 241
- Viewing Core Files from Junos OS Processes on page 242

Configuring Failover to Backup Media if a Junos OS Process Fails

For routers or switches with redundant Routing Engines, you can configure the router or switch to switch to backup media that contains a version of the system if a software process fails repeatedly. You can configure the router or switch 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.

Related Documentation

- Disabling Junos OS Processes on page 240
- Saving Core Files from Junos OS Processes on page 242
- **processes on page 410**

Configuring Password Authentication for 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 OS 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.

Related Documentation

- Configuring Password Authentication for Console Access to PICs on page 238

Viewing Core Files from Junos OS 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 files.

```
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
```

Related Documentation

- Saving Core Files from Junos OS Processes on page 242
- Saving Core Files Generated by Junos OS Processes

Saving Core Files from Junos OS 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 10.

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;
```

Related Documentation

- Viewing Core Files from Junos OS Processes on page 242

Using Junos OS to Configure Logical System Administrators

Using the Junos OS, you can partition a single router or switch into multiple logical devices that perform independent routing or switching 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.

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, switching statements, and policy statements for the logical system.

Related Documentation

- Defining Junos OS Login Classes on page 78
- Defining Junos OS Login Classes

Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site

You can configure a router or switch to transfer its configuration to an archive file periodically. Tasks to configure the configuration transfer to an archive site are:

1. Configuring the Router or Switch to Transfer Its Currently Active Configuration to an Archive on page 244
2. Configuring the Transfer Interval for Periodic Transfer of the Active Configuration to an Archive Site on page 244

Configuring the Router or Switch to Transfer Its Currently Active Configuration to an Archive

If you want to back up your device's current configuration to an archive site, you can configure the router or switch to transfer its currently active configuration by FTP or secure copy (SCP) periodically or after each commit.

To configure the router or switch to transfer its currently active configuration to an archive site, include statements at the **[edit system archival configuration]** hierarchy level:

```
[edit system archival configuration]
archive-sites {
  ftp://username<:password>@host-address<:port>/url-path;
  scp://username<:password>@host-address<:port>/url-path;
}
transfer-interval interval;
transfer-on-commit;
```

NOTE: When specifying a URL in a Junos OS 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*"**

Configuring the Transfer Interval for Periodic Transfer of the Active Configuration to an Archive Site

To configure the router or switch 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 of the Current Active Configuration When a Configuration Is Committed

To configure the router or switch 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 OS 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 Transfer of Active Configuration Files

When you configure the router or switch 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 or switch 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 an FTP URL, or 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;
  scp://username@host:<port>url-path password password;
  file://<path>/<filename>;
}
```

NOTE: When specifying a URL in a Junos OS 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 or switch is UTC.

Using Junos OS to Specify the Number of Configurations Stored on the CompactFlash Card

By default, the Junos OS saves the current configuration and three previous versions of the committed configuration on the CompactFlash card. The currently operational Junos OS 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 or switch'sCompactFlash 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.

Related Documentation

- Configuring Automatic Mirroring of the CompactFlash Card on the Hard Disk Drive on page 68
- max-configurations-on-flash

Configuring RADIUS System Accounting

With RADIUS accounting enabled, Juniper Networks routers or switches, 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.

Tasks for configuring RADIUS system accounting are:

Configuring Auditing of User Events on a RADIUS Server

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;
      }
    }
  }
}
```


Specifying RADIUS Server Accounting and Auditing Events

To specify the events you want to audit when using a RADIUS server for authentication, 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 Server 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 OS 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 or switch 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 or switch interfaces.

Optionally, you can specify the number of times that the router or switch attempts to contact a RADIUS authentication server by including the **retry** statement. By default, the router or switch retries three times. You can configure the router or switch to retry from 1 through 10 times.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a RADIUS server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

Example: Configuring RADIUS System 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;
        }
      }
    }
  }
}
```

Related Documentation

- Configuring RADIUS System Accounting on page 246

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;
      }
    }
  }
}
```

Tasks for configuring TACACS+ system accounting are:

1. Specifying TACACS+ Auditing and Accounting Events on page 249
2. Configuring TACACS+ Server Accounting on page 249

Specifying TACACS+ Auditing and Accounting Events

To specify the events you want to audit when using a TACACS+ server for authentication, 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+ Server 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 OS 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 or switch 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 or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch 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);
```

Related Documentation

- Configuring TACACS+ Accounting on a TX Matrix Router on page 250
- Configuring TACACS+ Authentication on page 108

Configuring TACACS+ Accounting on a TX Matrix Router

On a TX Matrix router, 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 router, control is done under the switch-card chassis only.

Related Documentation

- Configuring TACACS+ System Accounting on page 248

Configuring the Junos OS to Work with SRC Software

You can enable Junos OS to work with the Session and Resource Control (SRC) software. The SRC software supports dynamic service activation engine (SAE) functionality on routers and switches running under Junos OS. 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 or switch is established, the SRC process (sdxd) starts a Junos XML protocol session as **user root**. You have the option of configuring **user sdx** with a different classification at the **[edit system login]** hierarchy level.

For more information about SRC software, see the SRC documentation set.

Related Documentation

- Configuring Finger Service for Remote Access to the Router on page 224
- Configuring FTP Service for Remote Access to the Router or Switch on page 225
- Configuring SSH Service for Remote Access to the Router or Switch on page 226
- Configuring Outbound SSH Service on page 227
- Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 231
- Configuring Telnet Service for Remote Access to a Router or Switch on page 232
- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189

Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages

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 number of seconds in the rate-limiting bucket. The packet rate is the rate-limiting packets earned per second. Specify a **bucket-size** from 0 through 4294967295 seconds. The default value is 5 seconds. Specify a **packet-rate** from 0 through 4,294,967,295. The default value is 1000.

Related Documentation

- Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 252

Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages

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 rate-limiting packets earned per second. Specify a **bucket-size** from 0 through 4294967295 seconds. The default value is 5 seconds. Specify a **packet-rate** from 0 through 4294967295. The default value is 1000.

Related Documentation

- Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 251

Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections

By default, path maximum transmission unit (MTU) discovery on outgoing IP-IP tunnel connections is enabled.

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;
```

To reenable 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;
```

Related Documentation

- Configuring the Junos OS for IPv6 Path MTU Discovery on page 254
- Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 255
- Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 256
- **ipip-path-mtu-discovery on page 370**

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.

The following sections describe how to configure TCP MSS on T Series and M Series routers and J Series Services Routers, respectively:

1. Configuring TCP MSS on T Series and M Series Routers on page 253
2. Configuring TCP MSS on J Series Services Routers on page 253

Configuring TCP MSS on T Series and M Series Routers

To specify a TCP MSS value on T Series and M Series routers, include the **tcp-mss** statement at the **[edit services service-set *service-set-name*]** hierarchy level:

```
[edit services service-set service-set-name]
tcp-mss mss-value;
interface-service {
  service-interface sp-fpc/pic/port;
}
```

The range of the **tcp-mss *mss-value*** parameter is from 536 through 65535.

To view statistics of SYN packets received and SYN packets whose MSS value is modified, issue the **show services service-sets statistics tcp-mss** operational mode command.

For further information about configuring TCP MSS on T Series and M Series routers, see the *Junos OS Services Interfaces Configuration Guide*.

Configuring TCP MSS on J Series Services Routers

To specify a TCP MSS value on a J Series Services Router, include the following statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
tcp-mss {
  mss-value;
}
```

The range of the ***mss-value*** parameter is from 64 through 65535.

To remove the TCP MSS specification, use the following command:

```
delete system internet-options tcp-mss
```

For more information about configuring TCP MSS and session negotiation on J Series Services Routers, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Related Documentation

- Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 257
- Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 257

Configuring the Junos OS for 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*.

Related Documentation

- Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 252
- Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 255
- Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 256

Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts

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.

Related Documentation

- Junos OS Support for IPv6 Routing Protocols on page 13
- Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 254
- Configuring the Junos OS for IPv6 Path MTU Discovery on page 254

Configuring the Junos OS for Acceptance of IPv6 Packets with a 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 or switch. 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.

```
[edit system internet-options]
```

```
no-ipv6-reject-zero-hop-limit;
```

Related Documentation

- Configuring the Junos OS for IPv6 Path MTU Discovery on page 254
- Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts on page 254

Configuring the Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses

By default, the Junos OS disables the processing of IPv4-mapped IPv6 packets to protect against malicious packets from entering the network. This might result in IPv6 packets from being dropped in a pure IPv4 routing environment. In a mixed routing environment of IPv4 and IPv6 networks, you might want to enable the processing of IPv4-mapped IPv6 packets to ensure smooth packet flow. In addition, this might also be helpful when you are in the process of transitioning your routing environment from IPv4 to IPv6 networks.

To enable the processing of such IPv4-mapped IPv6 packets, include the **allow-v4mapped-packets** statement at the **[edit system]** hierarchy level:

```
[edit system]
allow-v4mapped-packets;
```

NOTE: We recommend that you configure this statement only after fully understanding the security implications of allowing IPv4-mapped IPv6 packets in your network.

Related Documentation

- allow-v4mapped-packets on page 298

Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections

By default, path MTU discovery on outgoing GRE tunnel connections is enabled. 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;
```

To reenable 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;
```

Related Documentation

- Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 256

Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections

By default, path MTU discovery on outgoing TCP connections is enabled. To disable path MTU discovery, include the **no-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-path-mtu-discovery;
```

To reenable path MTU discovery on outgoing TCP connections, include the **path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
path-mtu-discovery;
```

Related Documentation

- Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 255
- Configuring the Junos OS to Ignore ICMP Source Quench Messages on page 256

Configuring the Junos OS to Ignore ICMP Source Quench Messages

By default, Internet Control Message Protocol (ICMP) source quench is disabled. You enable **source quench** when you want the Junos OS 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;
```

Related Documentation

- Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 251
- Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 252

Configuring the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set

By default, the router or switch accepts packets that have both the SYN and FIN bits set in the TCP flag. You can configure the router or switch 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 or switch 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;
```

Related Documentation

- Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 257
- Configuring the Junos OS to Extend the Default Port Address Range on page 257

tcp-drop-synfin-set on page 443

Configuring the Junos OS to Disable 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;
```

Related Documentation

- Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 257
- Configuring the Junos OS to Extend the Default Port Address Range on page 257

no-tcp-rfc1323 on page 390

Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension

To configure the Junos OS 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;
```

Related Documentation

- Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 257
- Configuring the Junos OS to Extend the Default Port Address Range on page 257
- **no-tcp-rfc1323 on page 390**

Configuring the Junos OS to Extend the Default Port Address Range

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 configure the Junos OS to extend the default port address range, 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.

Related Documentation

- Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 257
- Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 258
- **source-port on page 434**
- source-port

Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses

The Address Resolution Protocol (ARP) is a protocol used by IPv4 to map IP network addresses to MAC addresses. This topic describes how to set passive ARP learning and ARP aging options for network devices. (A switch operates as a virtual router.)

Tasks for configuring ARP learning and aging are:

1. Configuring Passive ARP Learning for Backup VRRP Routers or Switches on page 258
2. Configuring a Delay in Gratuitous ARP Requests on page 259
3. Configuring a Gratuitous ARP Request When an Interface is Online on page 259
4. Configuring the Purging of ARP Entries on page 259
5. Adjusting the ARP Aging Timer on page 259

Configuring Passive ARP Learning for Backup VRRP Routers or Switches

By default, the backup VRRP router or switch drops ARP requests for the VRRP-IP to VRRP-MAC address translation. The backup router or switch 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 or switch and becomes the new master, the backup router or switch must learn all the entries that were present in the ARP cache of the master router or switch. In environments with many directly attached hosts, such as metro Ethernet environments (this type of environment does not pertain to switches), 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 or switch to hold approximately the same contents as the ARP cache in the master router or switch, 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 or switches. This prevents the need to intervene manually when the master router or switch becomes the backup router or switch. While a router or switch is operating as the master, the passive learning configuration has no operational impact. The configuration takes effect only when the router or switch is operating as a backup router or switch.

Configuring a Delay in Gratuitous ARP Requests

By default, the Junos OS sends gratuitous ARP requests immediately after configuration changes are made on an interface. This might lead to the Packet Forwarding Engine dropping some initial request packets if the configuration updates have not been fully processed. To avoid such request packets from being dropped, you can configure a delay in gratuitous ARP requests.

To configure a delay in gratuitous ARP requests, include the **gratuitous-arp-delay** ***seconds*** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]
gratuitous-arp-delayseconds;
```

We recommend that you configure a value in the range of **3** through **6** seconds.

Configuring a Gratuitous ARP Request When an Interface is Online

To configure the Junos OS to automatically send a gratuitous ARP request when an interface is online, include the **gratuitous-arp-on-ifup** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]
gratuitous-arp-on-ifup;
```

Configuring the Purging of ARP Entries

To configure the purging of obsolete ARP entries in the cache when an interface goes offline, include the **purging** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]
purging;
```

NOTE: Purging is configured to delete ARP entries immediately after an interface that has gone offline is detected. If purging is not configured, ARP entries in the ARP table are retried after they have expired and are deleted if there is no ARP response within the default timeout value of 20 minutes. The default timeout value can be configured to other values using the **aging-timer** statement.

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 in an event where having thousands of clients time out at the same time might impact packet forwarding performance. In environments where there are devices connected with lower ARP aging timers (less than 20 minutes), decreasing the ARP aging timer can improve performance by preventing the flooding of traffic toward next hops with expired ARP entries. In most environments, the default ARP aging timer value does not need to be adjusted.

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 **aging-timer** statement and the timer value in minutes at the **[edit system arp interfaces *interface-name*]** hierarchy level:

```
[edit system arp interfaces 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.

Related Documentation

- Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors on page 260

Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors

The Junos OS provides the **no-neighbor-learn** configuration statement at the **[edit interfaces *interface-name* unit *interface-unit-number* family inet]** and **[edit interfaces *interface-name* unit *interface-unit-number* family inet6]** hierarchy levels.

To disable ARP address learning by not sending arp-requests and not learning from ARP replies for IPv4 neigbors, include the **no-neighbor-learn** statement at the **[edit interfaces *interface-name* unit *interface-unit-number* family inet**] hierarchy level:

```
[edit interfaces interface-name unit interface-unit-number family inet]
no-neighbor-learn;
```

To disable neighbor discovery for IPv6 neighbors, include the **no-neighbor-learn** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet6]** hierarchy level:

```
[edit interfaces interface-name unit interface-unit-number family inet6]
no-neighbor-learn;
```

Related Documentation

- Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 258

Configuring System Alarms to Appear Automatically on J Series Routers, EX Series Ethernet Switches, and the QFX Series

You can configure J Series routers, EX Series switches, and the QFX Series to execute a **show system alarms** command whenever a user with the login class **admin** logs in to the router or switch. To do so, include the **login-alarms** statement at the **[edit system login class admin]** hierarchy level.

```
[edit system login class admin]
login-alarms;
```

For more information on the **show system alarms** command, see the *Junos OS System Basics and Services Command Reference*.

Related Documentation

- System Alarms on J Series Routers on page 261
- show system alarms

System Alarms on J Series Routers

Table 32 on page 261 describes system alarms that may occur on J Series routers. These alarms are preset and cannot be modified.

Table 32: System Alarms on J Series Routers

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 enables management access to the router.	Create the rescue configuration.
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.

Related Documentation

- Configuring System Alarms to Appear Automatically on J Series Routers, EX Series Ethernet Switches, and the QFX Series on page 261

CHAPTER 12

Security Configuration Example

This chapter includes the following topics:

Example: Configuring a Router Name and Domain Name

The following example shows how to configure the router's name and domain name:

```
[edit]
system {
  host-name Secure-Router;
  domain-name company.com;
  default-address-selection;
}
```

Related Documentation

- Configuring the Hostname of the Router or Switch on page 62

Example: Configuring RADIUS Authentication

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and 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.

The Junos OS uses one or more template accounts to perform user authentication. You create the template account or accounts, and then configure the user access to use that account. If the RADIUS server is unavailable, the fallback is for the login process to use the local account that set up on the router or switch.

The following example shows how to configure RADIUS authentication:

```
[edit]
system {
  authentication-order [ radius password ];
  root-authentication {
    encrypted-password "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; # SECRET-DATA
  }
  name-server {
    10.1.1.1;
    10.1.1.2;
  }
}
```

The following example shows how to enable RADIUS authentication and define the shared secret between the client and the server. The secret enables the client and server to determine that they are talking to the trusted peer.

Define a timeout value for each server, so that 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;
    }
  }
}
```

Related Documentation

- Configuring RADIUS Authentication on page 103

Example: Creating Login Classes

The following example shows how to 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;
      }
   }
}
```

Related Documentation

- Defining Junos OS Login Classes on page 78
- Defining Junos OS Login Classes

Example: Configuring User Login Accounts

The following example shows how to configure the local admin account. If RADIUS fails or becomes unreachable, the login proccess reverts to password authentication on the local accounts on the router or switch.

```
[edit]
system {
   login {
      user admin {
         uid 1000;
         class engineering;
         authentication {
            encrypted-password "<PASSWORD>"; # SECRET-DATA
         }
```



```
        }
    }
}
```

Related Documentation

- Configuring Junos OS User Accounts on page 81

Example: Configuring RADIUS Template Accounts

The following example shows how to configure 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;
        }
    }
}
```

Related Documentation

- Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 112

Example: Enabling SSH Connection Services

The following example shows how to 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 OS. 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;
    }
}
```

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 226

Example: Configuring System Logging

The system log file records when authentication and authorization is granted and rejected, and what user commands are executed. It 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.

The following example shows how to configure a 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;
      }
   }
}
```

Related Documentation

- Junos OS System Log Configuration Overview on page 139

Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

Debugging and troubleshooting are much easier when the timestamps in the log files of all the routers or switches are synchronized, because events that span the network can be correlated with synchronous entries in multiple logs. We strongly recommend using the Network Time Protocol (NTP) to synchronize the system clocks of routers, switches, and other network equipment.

By default, NTP operates in an entirely unauthenticated manner. If a malicious attempt to influence the accuracy of a router or switch'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 sample configuration synchronizes all the routers or switches 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 should be used to hash the key value for authentication, which prevents the router or switch from synchronizing with an attacker's host posing as the time server.

```
[edit]
system {
  ntp {
    authentication-key 2 type md5 value "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; # SECRET-DATA
    boot-server 10.1.4.1;
    server 10.1.4.2;
  }
}
```

Related Documentation

- NTP Overview on page 128
- NTP Time Server and Time Services Overview on page 131

- authentication-key
- boot-server
- server
- show ntp associations
- show ntp status

Example: Configuring ATM, SONET, Loopback, and Out-of-Band Management Interfaces

The following example shows how to configure the interfaces on your router. It covers configurations for Asynchronous Transfer Mode (ATM), SONET, loopback, and out-of-band management interfaces.

The following example shows how to 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.

The following example shows how to configure an **fxp0** interface as a loopback interface:

```
[edit]
interfaces {
    fxp0 {
        disable;
    }
}
```

The following example shows how to configure the loopback interface and apply a firewall filter to protect the Routing Engine. 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;
            }
        }
    }
}
```

The following example shows how to 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;
        }
```

```
  }
}
```

Example: Configuring SNMPv3

The following example shows how to configure Simple Network Management Protocol version 3 (SNMPv3) on a router running Junos OS:

```
[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
}
}
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;
    }
  }
```

Examples: Configuring Protocol-Independent Routing Properties

This section includes the following topics:

Example: Configuring the Router ID and Autonomous System Number for BGP

The following example shows how to configure a router ID and autonomous system (AS) number for the Border Gateway Protocol (BGP):

```
[edit]
routing-options {
  router-id 10.1.7.1;
  autonomous-system 222;
}
```

Related Documentation

- Example: Configuring Martian Addresses on page 273
- Example: Viewing Reserved IRI IP Addresses on page 273
- Example: Configuring the BGP and IS-IS Routing Protocols on page 274

Example: Configuring Martian Addresses

The following example shows how to configure martian addresses, which are reserved host or network addresses about which all routing information should be ignored. By default, the Junos OS 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;
  }
}
```

Related Documentation

- Example: Viewing Reserved IRI IP Addresses on page 273

Example: Viewing 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.

The following example shows how to use the CLI command **show route table __juniper_private1__** to view the router's configured IP addresses, including the reserved IRI IP addresses.

```
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
```

Related Documentation

- Example: Configuring Martian Addresses on page 273

Example: Configuring the BGP and IS-IS 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 OS 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 the following examples, we configure BGP as the exterior gateway protocol (EGP) and IS-IS as the interior gateway protocol (IGP). If you use OSPF, configure it similarly to the IS-IS configuration shown.

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 trade-off 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 "$9$aH1j8gqQ1gjyjgjhgjgiiiii";
    }
    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 "$9$aH1j8gqQ1gjyjgjhgjgiiiii";
    }
  }
}
```

Configuring IS-IS

Although all IGPs supported by the Junos OS 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.

The following example also shows how to configure 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 "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; # 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;
    }
  }
}
```

Related Documentation

- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 637

Configuring Firewall Policies and Filters

Example: Configuring Firewall Filters

The following example shows how to configure a firewall filter to protect 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;
            }
          }
        }
      }
    }
```

Related Documentation

- Example: Configuring Firewall Policies on page 280
- Example: Consolidated Security Configuration on page 281

Example: Configuring Firewall Policies

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.

The following example shows how to configure firewall policies:

```
[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;
    }
}
```

Related Documentation

- Example: Configuring Firewall Filters on page 277
- Example: Consolidated Security Configuration on page 281

Example: Consolidated Security Configuration

This topic provides a complete example of configuring various security features available in the Junos OS to secure your router:

Configuring Basic System Information

```
system {
    host-name Secure-Router;
    domain-name company.com;
    default-address-selection;
}
```

Configuring RADIUS Authentication

```
authentication-order [ radius password ];
root-authentication {
    encrypted-password "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; # 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;
    }
}
```

Configuring 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;
  }
}
```

Configuring User Login Accounts

```
user admin {
  uid 1000;
  class engineering;
  authentication {
    encrypted-password "<PASSWORD>"; # SECRET-DATA
  }
}
```

Configuring RADIUS Template Accounts

```
user observation {
  uid 1001;
  class observation;
}
user operation {
  uid 1002;
  class operation;
}
user engineering {
  uid 1003;
  class engineering;
}
```

Configuring SSH Connection Services

```
services {
  ssh connection-limit 10 rate-limit 4;
}
```

Configuring 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;
  }
}
```

Configuring the Time Source

```
ntp {
  authentication-key 2 type md5 value "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; \
  #  SECRET-DATA
  boot-server 10.1.4.1;
  server 10.1.4.2;
}
```


Configuring 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;
    }
  }
}
```

Configuring 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
        # will be sent. In this case, include 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 snmpv3 snmp-community community-index] 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;
      }
    }
  }
```

Configuring the Router ID and AS Number for BGP

```
[edit]
  routing-options {
  router-id 10.1.7.1;
  autonomous-system 222;
}
```

Configuring 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;
  }
}
```

Configuring 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 "$9$aH1j8gqQ1gjyjgjhgjgiiiii";
  }
  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 "$9$aH1j8gqQ1gjyjgjhgjgiiiii";
  }
}
```

Configuring IS-IS

```
isis {
  authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; # 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 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;
  }
}
```

Configuring 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;
    }
}
```

Related Documentation

- Example: Configuring Firewall Filters on page 277
- Example: Configuring Firewall Policies on page 280

CHAPTER 13

Summary of System Management Configuration Statements

The following topics 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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure audit of TACACS+ or RADIUS authentication events, configuration changes, and interactive commands.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS System Accounting on page 246
- Configuring TACACS+ System Accounting on page 248

access-end

Syntax access-end *HH*:*MM*;

Hierarchy Level [edit system **login** class]

Release Information Statement introduced in Junos OS Release 10.1.

Description Configure the end time for login access.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Time-Based User Access on page 84

access-start

Syntax access-start *HH*:*MM*;

Hierarchy Level [edit system **login** class]

Release Information Statement introduced in Junos OS Release 10.1.

Description Configure the start time for login access.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Time-Based User Access on page 84

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication on page 103
- Configuring RADIUS System Accounting on page 246

allow-commands

Syntax allow-commands "*regular-expression*";

Hierarchy Level [edit system login **class** *class-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying Access Privileges for Junos OS Operational Mode Commands on page 92
- **deny-commands on page 331**
- **user on page 464**

allow-configuration-regexps

Syntax allow-configuration-regexps "*regular expression 1*" "*regular expression 2*" ....;

Hierarchy Level [edit system login **class** *class-name*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Explicitly allow configuration access to specified hierarchies using regular expressions even if the permissions set with the **permissions** statement do not allow that access. Configure multiple regular expressions as a string, separating each expression with standard delimiters such as white spaces or commas.

The statement **deny-configuration-regexps** takes precedence if it is used in the same login class definition.

Default If you do not configure this statement or the **deny-configuration-regexps** statement, users can edit only those commands for which they have access privileges set with 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. Enter as many expressions as needed, separating each with standard field delimiters such as white spaces or commas.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 96
- Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 100
- **deny-configuration-regexps on page 332**
- **user on page 464**

allow-v4mapped-packets

Syntax allow-v4mapped-packets;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 10.4.

Description Enable the processing of IPv4-mapped IPv6 packets.

Options None

Default: IPv4-mapped IPv6 address processing is disabled.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses on page 255

allowed-days

Syntax allowed-days [*days-of-the-week*];

Hierarchy Level [edit system **login** class *class-name*]

Release Information Statement introduced in Junos OS Release 10.1.

Description Specify the days of the week when users can log in.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Time-Based User Access on page 84

announcement

Syntax announcement *text*;

Hierarchy Level [edit system login]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration

Related Documentation

- Configuring the Junos OS to Display a System Login Announcement on page 240
- **message on page 382**

archival

Syntax

```
archival {
  configuration {
    archive-sites {
      file://<path>/<filename>;
      ftp://username@host:<port>url-path password password;
      scp://username@host:<port>url-path password password;
    }
    transfer-interval interval;
    transfer-on-commit;
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure copying of the currently active configuration to an archive site. An archive site can be a file, or an FTP or SCP location.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site on page 243

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure archiving properties for all system log files.

Options **files** ***number***—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file ***logfile***, it closes the file, compresses it, and renames it ***logfile*.0.gz** (the amount of data is determined by the **size** statement at this hierarchy level). 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).

Range: 1 through 1000

Default: 10 files

size ***size***—Maximum amount of data that the Junos OS 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***.

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 routers; 1 MB for M Series, MX Series, and T Series routers, and the QFX3500 switch; 10 MB for TX Matrix and TX Matrix Plus routers

world-readable | no-world-readable—Grant all users permission to read archived log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default: no-world-readable

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 156

archive (Individual System Log File)

Syntax archive <archive-sites (*ftp-url* <password *password*>)> <files *number*> <size *size*> <start-time "*YYYY-MM-DD.hh:mm*"> <transfer-interval *minutes*> <world-readable | no-world-readable>;

Hierarchy Level [edit system **syslog file** *filename*]

Release Information Statement introduced before Junos OS Release 7.4.
start-time and **transfer-interval** statements introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure archiving properties for a specific system log file.

Options **archive-sites** ***site-name***—FTP URL representing the destination for the archived log file (for information about how to specify valid FTP URLs, see "Format for Specifying Filenames and URLs in Junos OS CLI Commands" on page 46). 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.

files ***number***—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file ***logfile***, it closes the file, compresses it, and renames it ***logfile*.0.gz** (the amount of data is determined by the **size** statement at this hierarchy level). 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).

Range: 1 through 1000

Default: 10 files

password ***password***—Password for authenticating with the site specified by the **archive-sites** statement.

size ***size***—Maximum amount of data that the Junos OS 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***.

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 routers; 1 MB for M Series, MX Series, and T Series routers, and the QFX3500 switch; 10 MB for TX Matrix and TX Matrix Plus routers

start-time "*YYYY-MM-DD.hh:mm*"—Date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

transfer-interval ***interval***—Interval at which to transfer the log file to an archive site.

Range: 5 through **2880** minutes

world-readable | no-world-readable—Grant all users permission to read archived log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default: no-world-readable

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 156

archive-sites (Configuration File)

Syntax

```
archive-sites {
  file://<path>/<filename>;
  ftp://username@host:<port>url-path password password;
  scp://username@host:<port>url-path password password;
}
```

Hierarchy Level [edit system archival configuration]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify where to transfer the current configuration files. When specifying a URL in a Junos OS 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 or switch 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 or switch is configured as UTC or the local time zone. The default time zone on the router or switch is UTC.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Archive Sites for Transfer of Active Configuration Files on page 245
- **configuration on page 323**
- **transfer-on-commit on page 462**

arp

Syntax

```
arp {
  aging-timer minutes;
  gratuitous-arp-delayseconds;
  gratuitous-arp-on-ifup;
  interfaces {
    interface-name {
      aging-timer minutes;
    }
  }
  passive-learning;
  purging;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 **aging-timer**—Time interval in minutes between ARP updates. In environments where the number of ARP entries to update is high (for example, on routers only, metro Ethernet environments), increasing the time between updates can improve system performance.

Default: 20 minutes

Range: 5 to 240 minutes

The remaining 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 Documentation

- Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 258
- *Junos OS Network Interfaces Configuration Guide*

authentication (DHCP Local Server)

Syntax

```
authentication {
  password password-string;
  username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-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 dhcpv6**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services **dhcp-local-server dhcpv6 group** *group-name*],
[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 dhcpv6**],
[edit logical-systems *logical-system-name* system services **dhcp-local-server dhcpv6 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**],
[edit routing-instances *routing-instance-name* system services **dhcp-local-server dhcpv6**],
[edit routing-instances *routing-instance-name* system services **dhcp-local-server dhcpv6 group** *group-name*],
[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 dhcpv6**],
[edit system services **dhcp-local-server dhcpv6 group** *group-name*],
[edit system services **dhcp-local-server group** *group-name*]

Release Information

Statement introduced in Junos OS 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 remaining 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 Documentation
- Using External AAA Authentication Services with DHCP

authentication (Login)

Syntax

```
authentication {
  (encrypted-password "password" | plain-text-password);
  load-key-file file-name;
  ssh-dsa "public-key";
  ssh-rsa "public-key";
}
```

Hierarchy Level [edit system login user *username*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Authentication methods that a user can use to log in to the router or switch. You can assign multiple authentication methods to a single user.

Options

encrypted-password "*password*"—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.

load-key-file—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.

plain-text-password—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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Junos OS User Accounts on page 81
- **root-authentication on page 418**

authentication-key

Syntax authentication-key *key-number* type *type* value *password*;

Hierarchy Level [edit system **ntp**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure Network Time Protocol (NTP) authentication keys so that the router or switch can send authenticated packets. If you configure the router or switch 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring NTP Authentication Keys on page 134
- **broadcast on page 316**
- **peer on page 400**
- **server on page 424**
- **trusted-key on page 463**

authentication-order

Syntax authentication-order [*authentication-methods*];

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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**—Use the password configured for the user with the **authentication** statement at the **[edit system login user]** hierarchy level.
- **radius**—Use RADIUS authentication services.
- **tacplus**—Use TACACS+ authentication services.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 121
- **authentication on page 307**

autoinstallation

Syntax

```
autoinstallation {
  configuration-servers {
    url;
  }
  interfaces {
    interface-name {
      bootp;
      rarp;
    }
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Download a configuration file automatically from an FTP, Hypertext Transfer Protocol (HTTP), or Trivial FTP (TFTP) server. When you power on a router or switch configured for autoinstallation, it requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server. Once the router or switch has an address, it sends a request to a configuration server and downloads and installs a configuration.

Options The remaining 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 Documentation

- Upgrading Software Using Automatic Software Download on EX Series Switches
- *J Series Services Router Basic LAN and WAN Access Configuration Guide*
- **configuration-servers on page 324**
- **idle-timeout on page 363**

auxiliary

Syntax

```
auxiliary {
  disable;
  insecure;
  type terminal-type;
}
```

Hierarchy Level [edit system **ports**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the characteristics of the auxiliary port.

Default The auxiliary port is disabled.

Options **disable**—Disable the port.

insecure—Disable super user access or root logins to establish terminal connection.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Set Console and Auxiliary Port Properties on page 234

backup-router

Syntax backup-router *address* <destination *destination-address*>;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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 OS 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.

NOTE: **The Routing Engine on the backup router only supports 16 destinations addresses. If you configure more than 16 destination addresses, the Junos OS ignores destination addresses after the sixteenth address and displays a commit-time warning message to this effect.**

Default: All hosts (default route) are reachable through the backup router.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring a Backup Router on page 66

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190
- **boot-server on page 314**

boot-server (DHCP)

Syntax boot-server (*address* | *hostname*);

Hierarchy Level [edit system services **dhcp**],
[edit system services dhcp **pool**],
[edit system services dhcp **static-binding**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches 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***—IP address of a DHCP boot server.
- ***hostname***—Hostname of a DHCP boot server.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190
- **boot-file on page 313**

boot-server (NTP)

Syntax boot-server (*address* | *hostname*);

Hierarchy Level [edit system **ntp**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the server that NTP queries when the router or switch boots to determine the local date and time.

When you boot the router or switch, 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 or switch uses to determine the time when the router or switch 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 or switch's time. You can either configure an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the **ntpdate** request resolves the hostname to an IP address when the router or switch boots up.

Options

- ***address***—The IP address of an NTP boot server.
- ***hostname***—The hostname of an NTP boot server.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the NTP Boot Server on page 129

broadcast

Syntax broadcast *address* <key *key-number*> <version *value*> <ttl *value*>;

Hierarchy Level [edit system **ntp**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the local router or switch to operate in broadcast mode with the remote system at the specified ***address***. In this mode, the local router or switch 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 or switch 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

ttl *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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the NTP Time Server and Time Services on page 132

broadcast-client

Syntax broadcast-client;

Hierarchy Level [edit system **ntp**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the local router or switch to listen for broadcast messages on the local network to discover other servers on the same subnet.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router or Switch to Listen for Broadcast Messages Using NTP on page 135

change-type

Syntax change-type (character-sets | set-transitions);

Hierarchy Level [edit system login **password**]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Set requirements for using character sets in plain-text passwords. When you combine this statement 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 Specify 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Special Requirements for Junos OS Plain-Text Passwords on page 72
- **minimum-changes on page 383**

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 authentication**username-include**],
[edit system services dhcp-local-server group *group-name* authentication **username-include**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify that the circuit type is concatenated with the username during the subscriber authentication process.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services to Authenticate DHCP Clients on page 214

class (Assigning a Class to an Individual User)

Syntax class *class-name*;

Hierarchy Level [edit system login **user** *username*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Junos OS User Accounts on page 81

class (Defining Login Classes)

Syntax

```
class class-name {
  allow-commands "regular-expression";
  allow-configuration-regexps "regular expression1" "regular expression2";
  deny-commands "regular-expression";
  deny-configuration-regexps "regular expression1" "regular expression2";
  idle-timeout minutes;
  permissions [ permissions ];
}
```

Hierarchy Level [edit system **login**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Define a login class.

Options *class-name*—A name you choose for the login class.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Defining Junos OS Login Classes on page 78
- **user on page 464**

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

commit synchronize

Syntax commit synchronize;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For devices with multiple Routing Engines only. Configure a **commit** command to automatically result in a **commit synchronize** command. The Routing Engine on which you execute the **commit** command (the requesting Routing Engine) copies and loads its candidate configuration to the other (the 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.

Starting with Junos OS Release 9.3, accounting of events and operations on a backup Routing Engine is not supported on accounting servers such as TACACS+ or RADIUS. Logging of accounting events is supported only for events and operations on a master Routing Engine.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Multiple Routing Engines to Synchronize Committed Configurations Automatically on page 75

compress-configuration-files

Syntax (compress-configuration-files | no-compress-configuration-files);

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Compressing the Current Configuration File on page 75

configuration

Syntax

```
configuration {
  transfer-interval interval;
  transfer-on-commit;
  archive-sites {
    file://<path>/<filename>;
    ftp://<username>:<password>@<host>:<port>/<url-path> password password;
    http://username@host:<port>url-path password password;
    scp://username@host:<port>url-path password password;
  }
}
```

Hierarchy Level [edit system archival]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the router or switch to periodically transfer its currently active configuration (or after each commit).

Options The remaining 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 Documentation

- Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site on page 243
- **archive on page 301**
- **archive-sites on page 304**
- **transfer-interval on page 461**
- **transfer-on-commit on page 462**

configuration-servers

Syntax

```
configuration-servers {
  url;
}
```

Hierarchy Level [edit **system autoinstallation**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only, configure the URL address of a server from which to obtain configuration files. Examples of URLs:

tftp://*hostname/path/filename*

ftp://*username:prompt@ftp.hostname.net/filename /*

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Upgrading Software Using Automatic Software Download on EX Series Switches
- Getting Started Guide for your router model
- **autoinstallation on page 310**
- **idle-timeout on page 363**

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options

limit—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).

Range: **1** through **250**

Default: **75**

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189
- Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 223
- Configuring Finger Service for Remote Access to the Router on page 224
- Configuring FTP Service for Remote Access to the Router or Switch on page 225
- Configuring SSH Service for Remote Access to the Router or Switch on page 226
- Configuring Telnet Service for Remote Access to a Router or Switch on page 232

console (Physical Port)

Syntax

```
console {
  disable;
  insecure;
  log-out-on-disconnect;
  type terminal-type;
}
```

Hierarchy Level [edit system **ports**]

Release Information Statement introduced before Junos OS Release 7.4.
disable option added in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the characteristics of the console port.

Default The console port is enabled and its speed is 9600 baud.

Options **disable**—Disable console login connections.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Set Console and Auxiliary Port Properties on page 234

console (System Logging)

Syntax
```
console {
  facility severity;
}
```

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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 15 on page 146.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Table 16 on page 147.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Directing System Log Messages to the Console on page 149
- *Junos OS System Log Messages Reference*

default-address-selection

Syntax default-address-selection;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Use the loopback interface, **lo0**, as the source address for all locally generated IP packets when the packet is sent through a routed interface, but not when the packet is sent through a local interface such as **fxp0**. The **lo0** interface is the interface to the router's or switch's Routing Engine.

Default The default address is used as the source address for all locally generated IP packets on outgoing interfaces that are unnumbered. If an outgoing interface is numbered, the default address is chosen using the following sequence:

- The primary address on the loopback interface **lo0** that is *not* **127.0.0.1** is used.
- The primary address for the primary interface or the preferred address (if configured) for the primary interface is used.

  By default, the primary address on an interface is selected as the numerically lowest local address configured on the interface.

  An interface's *primary address* is used by default as the local address for broadcast and multicast packets sourced locally and sent out through the interface. An interface's *preferred address* is the default local address used for packets sourced by the local router or switch to destinations on the subnet. By default, the numerically lowest local address configured for the interface is chosen as the preferred address on the subnet.

  To configure a different primary address or preferred address, include the **primary** or **preferred** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family *family* address *address*** or **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family* address *address*** hierarchy levels.

  For more information about default, primary, and preferred addresses for an interface, see "Configuring Default, Primary, and Preferred Addresses and Interfaces" in the *Junos OS 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 Documentation

- Configuring the Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets on page 236
- *Junos OS Network Interfaces Configuration Guide*

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches 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 (1day)

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190
- **maximum-lease-time on page 381**

delimiter (DHCP Local Server)

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 dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services **dhcp-local-server dhcpv6 group** *group-name* **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 dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* system services **dhcp-local-server dhcpv6 group** *group-name* **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 dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services **dhcp-local-server dhcpv6 group** *group-name* **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 dhcpv6 authentication username-include**],
[edit routing-instances *routing-instance-name* system services **dhcp-local-server dhcpv6 group** *group-name* **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 authentication username-include**],
[edit system services **dhcp-local-server dhcpv6 authentication username-include**],
[edit system services **dhcp-local-server dhcpv6 group** *group-name* **authentication username-include**],
[edit system services **dhcp-local-server group** *group-name* **authentication username-include**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify the character used as the delimiter between the concatenated components of the username.

Options ***delimiter-character***—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services with DHCP

deny-commands

Syntax

deny-commands "*regular-expression*";

Hierarchy Level

[edit system login **class**]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying Access Privileges for Junos OS Operational Mode Commands on page 92
- **allow-commands on page 296**
- **user on page 464**

deny-configuration-regexps

Syntax deny-configuration-regexps "*regular expression 1*" "*regular expression 2*";

Hierarchy Level [edit system login **class** *class-name*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Explicitly deny configuration access to specified hierarchies using regular expressions even if the permissions set with the **permissions** statement allow that access. Configure multiple regular expressions as a string, separating each expression with standard delimiters such as white spaces or commas.

Expressions configured with this statement take precedence over **allow-configuration-regexps** if the two statements are used in the same login class definition.

Default If you do not configure this statement or the **deny-configuration-regexps** statement, users can edit only those commands for which they have access privileges set with 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. Enter as many expressions as needed, separating each with standard field delimiters such as white spaces or commas.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 96
- **allow-configuration-regexps on page 297**
- **user on page 464**

destination

Syntax

```
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 **accounting**]

Release Information

Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure the authentication server.

Options

The remaining 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 Documentation

- Configuring RADIUS System Accounting on page 246
- Configuring TACACS+ System Accounting on page 248

destination-override

Syntax

```
destination-override {
  syslog host ip-address;
}
```

Hierarchy Level [edit system tracing]

Release Information Statement introduced in Junos OS 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 These options specify the system logs and the host to which remote tracing output is sent:

- **syslog**—Specify the system process log files to send to the remote tracing host.
- **host** ***ip-address***—Specify the IP address to which to send tracing information.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Junos OS Tracing and Logging Operations on page 49
- Understanding Tracing and Logging Operations
- **tracing on page 460**

dhcp

Syntax

```
dhcp {
  boot-file filename;
  boot-server (address | hostname);
  default-lease-time seconds;
  domain-name domain-name;
  domain-search [domain-list];
  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-name 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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Configure a router, switch, 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190
- System Management Configuration Statements on page 53

dhcpv6

Syntax

```
dhcpv6 {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  group group-name {
    authentication {
    ...
    interface interface-name {
      exclude;
      overrides {
        interface-client-limit number;
      }
      trace;
      upto upto-interface-name;
    }
    overrides {
      interface-client-limit number;
    }
  }
  overrides {
    interface-client-limit number;
  }
}
```

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 OS Release 9.6.

Description

Configure DHCPv6 local server options on the router and enable the router to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access and accounting.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.

The remaining 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 Documentation
- DHCPv6 Local Server Overview

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;
    }
  }
  dhcpv6 {
    authentication {
      ...
    }
    group group-name {
      authentication {
        ...
      }
      interface interface-name {
        exclude;
        overrides {
          interface-client-limit number;
        }
        trace;
        upto upto-interface-name;
      }
      overrides {
        interface-client-limit number;
      }
    }
    overrides {
      interface-client-limit number;
    }
  }
  duplicate-clients-on-interface;
  dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
  forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
  group group-name {
    authentication {
      ...
    }
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
      primary-profile-name>;
    interface interface-name {
      exclude;
```

```
            overrides {
              client-discover-match <option60-and-option82>;
              interface-client-limit number;
              no-arp;
            }
            trace;
            upto upto-interface-name;
          }
          overrides {
            client-discover-match <option60-and-option82>;
            interface-client-limit number;
            no-arp;
          }
        }
        interface-traceoptions {
          file filename <files number> <match regular-expression > <size maximum-file-size>
            <world-readable | no-world-readable>;
          flag flag;
          no-remote-trace;
        }
        overrides {
          client-discover-match <option60-and-option82>;
          interface-client-limit number;
          no-arp;
        }
        pool-match-order {
          external-authority;
          ip-address-first;
          option-82;
        }
        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 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 OS 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 supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication. You can configure dynamic profile and authentication support on a global basis or for a specific group of interfaces.

The DHCP local server also supports the use of Junos 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 DHCP server on J Series routers and so is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, 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.

The **dhcpv6** stanza configures the router to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and 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 remaining 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 Documentation

- Extended DHCP Local Server Overview
- DHCPv6 Local Server Overview

diag-port-authentication

Syntax diag-port-authentication (encrypted-password "*password*" | plain-text-password);

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Password Authentication for the Diagnostics Port on page 241

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

domain-name

Syntax domain-name *domain-name*;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the name of the domain in which the router or switch 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Domain Name for the Router or Switch on page 64

domain-name (DHCP Local Server)

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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 authentication username-include**],
[edit system services dhcp-local-server **dhcpv6 authentication username-include**],
[edit system services dhcp-local-server dhcpv6 **group** *group-name* **authentication username-include**],
[edit system services dhcp-local-server **group** *group-name* **authentication username-include**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify the domain name that is concatenated with the username during the subscriber authentication process.

Options ***domain-name-string***—Domain name formatted string.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services with DHCP

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-binding]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 six domain names, with a total of up to 256 characters.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Domains to Search When a Router or Switch Is Included in Multiple Domains on page 65
- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

dump-device

Syntax

```
dump-device {
  compact-flash;
  removable-compact-flash;
  usb;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Getting Started Guide for your router model

events

Syntax events [*events*];

Hierarchy Level [edit system **accounting**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the types of events to track and log.

Options *events*—Event types; can be one or more of the following:

- **change-log**—Audit configuration changes.
- **interactive-commands**—Audit interactive commands (any command-line input).
- **login**—Audit logins.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying TACACS+ Auditing and Accounting Events on page 249

explicit-priority

Syntax explicit-priority;

Hierarchy Level [edit system syslog file *filename*],
[edit system syslog host]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Including Priority Information in System Log Messages on page 158
- *Junos OS System Log Messages Reference*
- **structured-data on page 438**

facility-override

Syntax facility-override *facility*;

Hierarchy Level [edit system syslog host]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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 18 on page 154.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Changing the Alternative Facility Name for Remote System Log Messages on page 151
- *Junos OS System Log Messages Reference*

file (System Logging)

Syntax

```
file filename {
  facility severity;
  archive {
    files number;
    size size;
    (no-world-readable | world-readable);
  }
  explicit-priority;
  match "regular-expression";
  structured-data {
    brief;
  }
}
```

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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 15 on page 146.

file ***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 of the specified level and higher are logged. For a list of the severities, see Table 16 on page 147.

The remaining 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 Documentation

- Directing System Log Messages to a Log File on page 147
- *Junos OS 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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for EX Series switches.

Description Configure the maximum number of archived log files to retain. When the Junos OS 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 156
- *Junos OS System Log Messages Reference*
- **size on page 432**

finger

Syntax

```
finger {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.

Description Allow finger requests from remote systems to the local router.

The remaining 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 Documentation

- Configuring Finger Service for Remote Access to the Router on page 224

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 OS Release 8.1.

Description Configure Dynamic Tasking Control Protocol (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**

Required Privilege Level flow-tap—To view this statement in the configuration.
flow-tap-control—To add this statement to the configuration.

Related Documentation

- Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 223

format

Syntax format (des | md5 | sha1);

Hierarchy Level [edit system login password]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the authentication algorithm for plain-text passwords.

Default For Junos OS, 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:

- **des**—Has a block size of 8 bytes; its key size is 48 bits long.
- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Special Requirements for Junos OS Plain-Text Passwords on page 72

ftp

Syntax

```
ftp {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Allow FTP requests from remote systems to the local router or switch.

Options The remaining 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 Documentation
- Configuring FTP Service for Remote Access to the Router or Switch on page 225

full-name

Syntax full-name *complete-name*;

Hierarchy Level [edit system login user]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Junos OS User Accounts on page 81
- **user on page 464**
- user

gratuitous-arp-on-ifup

Syntax gratuitous-arp-on-ifup;

Hierarchy Level [edit system arp]

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure the sending of a gratuitous ARP request when an interface is online.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 258

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 enabled.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 255

group (DHCP Local Server)

Syntax

```
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      relay-agent-interface-id
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
  interface interface-name {
    exclude;
    overrides {
      client-discover-match <option60-and-option82>;
      interface-client-limit number;
      no-arp;
    }
    trace;
    upto upto-interface-name;
  }
  overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    no-arp;
  }
}
```

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 dhcpv6**],
[edit logical-systems *logical-system-name* system services **dhcp-local-server**],
[edit logical-systems *logical-system-name* system services **dhcp-local-server dhcpv6**],
[edit routing-instances *routing-instance-name* system services **dhcp-local-server**],
[edit routing-instances *routing-instance-name* system services **dhcp-local-server dhcpv6**],
[edit system services **dhcp-local-server**],
[edit system services **dhcp-local-server dhcpv6**]

Release Information

Statement introduced in Junos OS 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.

The remaining 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 Documentation

- Extended DHCP Local Server Overview
- Grouping Interfaces with Common DHCP Configurations
- Using External AAA Authentication Services with DHCP
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces

host

Syntax

host (*hostname* | other-routing-engine) {
  facility severity;
  explicit-priority;
  facility-override *facility*;
  log-prefix *string*;
  match "*regular-expression*";
  source-address
  port
}

TX Matrix Router and EX Series Switches

host (*hostname* | other-routing-engine | scc-master) {
  facility severity;
  explicit-priority;
  facility-override *facility*;
  log-prefix *string*;
  match "*regular-expression*";
  source-address
  port
}

QFX Series

host (*hostname* {
  facility severity;
  explicit-priority;
  facility-override *facility*;
  log-prefix *string*;
  match "*regular-expression*";
  source-address
  port
}

TX Matrix Plus Router

host (*hostname* | other-routing-engine | sfc0-master) {
  facility severity;
  explicit-priority;
  facility-override *facility*;
  log-prefix *string*;
  match "*regular-expression*";
  source-address
  port
}

Hierarchy Level

[edit system syslog]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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 15 on page 146.

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.

other-routing-engine—Direct messages to the other Routing Engine on a router or switch with two Routing Engines installed and operational.

NOTE: **The other-routing-engine option is not applicable to the QFX Series.**

port—Port number of the remote syslog server that can be modified.

scc-master—(TX Matrix routers only) On a T640 router that is part of a routing matrix, direct messages to the TX Matrix router.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Table 16 on page 147.

sfc0-master—(TX Matrix Plus routers only) On a T1600 router that is part of a routing matrix, direct messages to the TX Matrix Plus router.

The remaining 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 Documentation

- Directing System Log Messages to a Remote Machine or the Other Routing Engine on page 150
- Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router on page 173
- Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router on page 183
- *Junos OS System Log Messages Reference*

host-name

Syntax host-name *hostname*;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Set the hostname of the router or switch.

Options *hostname*—Name of the router or switch.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Hostname of the Router or Switch on page 62

http

Syntax

```
http {
  interfaces [ interface-names ];
  port port;
}
```

Hierarchy Level [edit **system services web-management**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the 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 or Gigabit Ethernet interfaces only.

The remaining statement is explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Management Access for the EX Series Switch (J-Web Procedure)
- *J-Web Interface User Guide*
- **https on page 360**
- **port on page 405**
- **web-management on page 469**

https

Syntax

```
https {
  interfaces [ interface-names ];
  local-certificate name;
  port port;
}
```

Hierarchy Level [edit **system services web-management**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 or Gigabit 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 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 Documentation

- Configuring Management Access for the EX Series Switch (J-Web Procedure)
- *J-Web Interface User Guide*
- **http on page 359**
- **port on page 405**
- **web-management on page 469**

icmpv4-rate-limit

Syntax

```
icmpv4-rate-limit {
  bucket-size seconds;
  packet-rate pps;
}
```

Hierarchy Level [edit system **internet-options**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure rate-limiting parameters for ICMPv4 messages sent.

Options **bucket-size *seconds***—Number of seconds in the rate-limiting bucket.

Range: 0 through 4294967295 seconds

Default: 5

packet-rate *pps*—Rate-limiting packets earned per second.

Range: 0 through 4294967295 pps

Default: 1000

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 251

icmpv6-rate-limit

Syntax

```
icmpv6-rate-limit {
  bucket-size seconds;
  packet-rate packet-rate;
}
```

Hierarchy Level [edit system **internet-options**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure rate-limiting parameters for ICMPv6 messages sent.

Options **bucket-size *seconds***—Number of seconds in the rate-limiting bucket.

Range: 0 through 4294967295 seconds

Default: 5

packet-rate *pps*—Rate-limiting packets earned per second.

Range: 0 through 4294967295 pps

Default: 1000

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 252

idle-timeout

Syntax idle-timeout *minutes*;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For a login class, configure the maximum time that a session can be idle before the user is logged off the router or switch. 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 4294967295 minutes

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Timeout Value for Idle Login Sessions on page 101
- **user on page 464**

inet6-backup-router

Syntax inet6-backup-router *address* <destination *destination-address*>;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Set a default router (running IP version 6 [IPv6]) to use while the local router or switch (running IPv6) is booting and if the routing protocol processes fail to start. The Junos OS removes the route to this router or switch 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 or switch, but without the risk of installing a default route in the forwarding table.

Default: All hosts (default route) are reachable through the backup router.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring a Backup Router on page 66

interfaces (ARP Aging Timer)

Syntax

```
interfaces {
  interface-name {
    aging-timer minutes;
  }
}
```

Hierarchy Level [edit system **arp**]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the ARP aging timer in minutes for a logical interface of family type **inet**.

Options **aging-timer *minutes***—Time between ARP updates, in minutes.

Default: 20

Range: 1 through 240

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Adjusting the ARP Aging Timer on page 259

interface (DHCP Local Server)

Syntax

```
interface interface-name {
  exclude;
  overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    no-arp;
  }
  trace;
  upto upto-interface-name;
}
```

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* routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6 group** *group-name*],
[edit logical-systems *logical-system-name* system services dhcp-local-server **group** *group-name*],
[edit logical-systems *logical-system-name* system services dhcp-local-server **dhcpv6 group** *group-name*],
[edit routing-instances *routing-instance-name* system services dhcp-local-server **group** *group-name*],
[edit routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6 group** *group-name*],
[edit system services dhcp-local-server **group** *group-name*],
[edit system services dhcp-local-server **dhcpv6 group** *group-name*]

Release Information

Statement introduced in Junos OS Release 9.0.
Options **upto** and **exclude** introduced in Junos OS 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.

NOTE: DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see the *Junos OS MX Series 3D Universal Edge Routers Solutions Guide*.

Options

exclude—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

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***.

The remaining 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 Documentation

- Extended DHCP Local Server Overview
- Grouping Interfaces with Common DHCP Configurations
- Using External AAA Authentication Services with DHCP

interfaces

Syntax

```
interfaces {
  interface-name {
    bootp;
    rarp;
    slarp;
  }
}
```

Hierarchy Level [edit **system autoinstallation**]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches 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**—Send requests over serial interfaces with Frame Relay.

rarp—Send requests over Ethernet interfaces.

slarp—(On J Series Services Routers only) Send requests over serial interfaces with HDLC.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Upgrading Software Using Automatic Software Download on EX Series Switches
- *J Series Services Router Basic LAN and WAN Access Configuration Guide*
- **autoinstallation on page 310**

internet-options

Syntax

```
internet-options {
  (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;
  tcp-mss mss-value;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure system IP options to protect against certain types of DoS attacks.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 251
- Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 252
- Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 252
- Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 255
- Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 256
- Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts on page 254
- Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 254
- Configuring the Junos OS to Ignore ICMP Source Quench Messages on page 256

- Configuring the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set on page 256
- Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 257
- Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 257
- Configuring the Junos OS to Extend the Default Port Address Range on page 257
- Configuring TCP MSS on J Series Services Routers on page 253

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 OS 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 gateway IP address if one is present in the DHCP client PDU. If no gateway IP address 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use
- Extended DHCP Local Server Overview
- Address-Assignment Pools Overview

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 enabled.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 252
- **internet-options on page 368**

ipv6-duplicate-addr-detection-transmits

Syntax ipv6-duplicate-addr-detection-transmits;

Hierarchy Level [edit system **internet-options**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Control the number of attempts for IPv6 duplicate address detection.

Default The default value is 3.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts on page 254

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 OS Release 9.2.
Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Configure path MTU discovery for IPv6 packets:

- **ipv6-path-mtu-discovery**—IPv6 path MTU discovery is enabled.
- **no-ipv6-path-mtu-discovery**—IPv6 path MTU discovery is disabled.

Default IPv6 path MTU discovery is enabled.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for IPv6 Path MTU Discovery on page 254

ipv6-path-mtu-discovery-timeout

Syntax ipv6-path-mtu-discovery-timeout *minutes*;

Hierarchy Level [edit system **internet-options**]

Release Information Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description Set the IPv6 path MTU discovery timeout interval.

Options *minutes*—IPv6 path MTU discovery timeout.
Default: 10 minutes

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for IPv6 Path MTU Discovery on page 254

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 OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Enable and disable rejecting incoming IPv6 packets with a zero hop limit value in their header.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 254

load-key-file

Syntax load-key-file;

Hierarchy Level [edit system root-authentication],
[edit system login user *username* authentication]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the Root Password on page 70
- Configuring Junos OS User Accounts on page 81

local-certificate

Syntax local-certificate;

Hierarchy Level [edit system services service-deployment],
[edit system services web-management https],
[edit system services xnm-ssl]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Import or reference an SSL certificate.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189
- Generating SSL Certificates to Be Used for Secure Web Access
- Importing SSL Certificates for Junos XML Protocol Support on page 640

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Physical Location of the Router or Switch on page 69

log-prefix

Syntax log-prefix *string*;

Hierarchy Level [edit system syslog host]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Include a text string in each message directed to a remote destination.

Options ***string***—Text string to include in each message.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Adding a Text String to System Log Messages on page 155
- *Junos OS System Log Messages Reference*

logical-system-name (DHCP Local Server)

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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 authentication username-include**],
[edit system services dhcp-local-server **dhcpv6 authentication username-include**],
[edit system services dhcp-local-server dhcpv6 **group** *group-name* **authentication username-include**],
[edit system services dhcp-local-server **group** *group-name* **authentication username-include**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify that the logical system name be concatenated with the username during the subscriber authentication process. No logical system name is concatenated if the configuration is in the default logical system.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using External AAA Authentication Services with DHCP

login

Syntax

```
login {
  announcement text;
  class class-name {
    allow-commands "regular-expression";
    allow-configuration-regexps "regular expression 1" "regular expression 2";
    deny-commands "regular-expression";
    deny-configuration-regexps "regular expression 1" "regular expression 2";
    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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure user access to the router or switch.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Defining Junos OS Login Classes on page 78

login-alarms

Syntax login-alarms;

Hierarchy Level [edit system login class admin]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description For J Series Services Routers, EX Series switches, and the QFX Series only. Show system alarms automatically when an **admin** user logs in to the router or switch.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring System Alarms to Appear Automatically on J Series Routers, EX Series Ethernet Switches, and the QFX Series on page 261
- *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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Enable CLI tips at login.

Default Disabled.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring CLI Tips on page 102

mac-address (DHCP Local Server)

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 authentication username-include**],
[edit system services dhcp-local-server **group** *group-name* **authentication username-include**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication process.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using External AAA Authentication Services with DHCP

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify a text string that must (or must not) appear in a message for the message to be logged to a destination.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using Regular Expressions to Refine the Set of Logged Messages on page 162

max-configurations-on-flash

Syntax max-configurations-on-flash *number*;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using Junos OS to Specify the Number of Configurations Stored on the CompactFlash Card on page 245

maximum-lease-time

Syntax maximum-lease-time *seconds*;

Hierarchy Level [edit system services dhcp]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

An exception is that the dynamic BOOTP lease length can exceed the maximum lease length specified.

Options ***seconds***—The maximum number of seconds the lease can be held.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190
- **default-lease-time on page 329**

maximum-length

Syntax maximum-length *length*;

Hierarchy Level [edit system login passwords]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 OS, no maximum is set.

Options **length**—The maximum number of characters the password can include.

Range: 1 to 64 characters

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Special Requirements for Junos OS Plain-Text Passwords on page 72

message

Syntax message *text*;

Hierarchy Level [edit system login]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure a system login message. This message appears before a user logs in.

You can format the message using the following special characters:

- \n—New line
- \t—Horizontal tab
- \'—Single quotation mark
- \"—Double quotation mark
- \\—Backslash

Options *text*—Text of the message.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration

Related Documentation

- Configuring the Junos OS to Display a System Login Message on page 238
- **announcement on page 299**

minimum-changes

Syntax minimum-changes *number*;

Hierarchy Level [edit system login passwords]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 OS, 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Special Requirements for Junos OS Plain-Text Passwords on page 72
- **change-type on page 317**

minimum-length

Syntax minimum-length *length*;

Hierarchy Level [edit system login passwords]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the minimum number of characters required in plain-text passwords. Newly created passwords must meet this requirement.

Default For Junos OS, 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Special Requirements for Junos OS Plain-Text Passwords on page 72
- **maximum-length on page 381**

mirror-flash-on-disk

Syntax mirror-flash-on-disk;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Automatic Mirroring of the CompactFlash Card on the Hard Disk Drive on page 68

multicast-client

Syntax multicast-client <*address*>;

Hierarchy Level [edit system ntp]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For NTP, configure the local router or switch 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 or switch joins those multicast groups.

Default: 224.0.1.1.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Router or Switch to Listen for Multicast Messages Using NTP on page 135

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring a DNS Name Server for Resolving a Hostname into Addresses on page 65
- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

next-server

Syntax next-server *next-server*;

Hierarchy Level [edit system services dhcp],
[edit system services dhcp pool *pool-id*],
[edit system services dhcp static-binding *mac-address*]

Release Information Statement introduced in Junos OS Release 8.4.

Description (J Series Services Routers only) Specify the IP address for the next DHCP server used for communication after a DHCP boot client establishes initial contact.

Options *next-server*—The IP address of the DHCP server that is used as the “siaddr” in a DHCP protocol packet.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Next DHCP Server to Contact After a Boot Client Establishes Initial Communication on page 200

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 OS Release 8.1.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable the Routing Engine Response to Multicast Ping Packets on page 237

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 OS Release 9.4.
Statement introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the Junos OS to disable the reporting of the IP address in ping responses.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 237

no-ping-time-stamp

Syntax no-ping-time-stamp;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the Junos OS to disable the recording of timestamps in ping responses.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 237

no-redirects

Syntax no-redirects;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Disable the sending of protocol redirect messages by the router or switch.

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 or switch sends redirect messages.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable Protocol Redirect Messages on the Router or Switch on page 235
- *Junos OS 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-paws;

Hierarchy Level [edit system internet-options]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the Junos OS to disable the RFC 1323 Protection Against Wrapped Sequence (PAWS) number extension.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 257

no-tcp-rfc1323

Syntax no-tcp-rfc1323;

Hierarchy Level [edit system internet-options]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the Junos OS to disable RFC 1323 TCP extensions.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 257

ntp

Syntax

```
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 ];
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure NTP on the router or switch.

The remaining 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 Documentation

- Synchronizing and Coordinating Time Distribution Using NTP on page 129

option-60 (DHCP Local Server)

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 authentication **username-include**],
[edit system services dhcp-local-server group *group-name* authentication **username-include**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication process.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services with DHCP

option-82 (DHCP Local Server Authentication)

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 authentication **username-include**],
[edit system services dhcp-local-server group *group-name* authentication **username-include**]

Release Information Statement introduced in Junos OS 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 is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.

Options **circuit-id**—(Optional) Agent Circuit ID suboption (suboption 1).

remote-id—(Optional) Agent Remote ID suboption (suboption 2).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using External AAA Authentication Services with DHCP

option-82 (DHCP Local Server Pool Matching)

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 OS 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. This statement is supported for IPv4 address-assignment pools only.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use
- Extended DHCP Local Server Overview
- Address-Assignment Pools Overview

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 regex> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure a router or switch running the Junos OS behind a firewall to communicate with client management applications on the other side of the firewall.

Default To configure transmission of the router's or switch'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 or switch. Each **outbound-ssh** stanza represents a single outbound SSH connection. This attribute is not sent to the client.

device-id—Identifies the router or switch to the client during the initiation sequence.

keep-alive—(Optional) When configured, specifies that the router or switch send keepalive messages to the management server. To configure the keepalive message, you must set both the **timeout** and **retry** attributes.

reconnect-strategy—(Optional) Specify the method the router or switch uses to reestablish a disconnected outbound SSH connection. Two methods are available:

- **in-order**—Specify that the router or switch first attempt to establish an outbound SSH session based on the management server address list. The router or switch attempts to establish a session with the first server on the list. If this connection is not available, the router or switch attempts to establish a session with the next server, and so on down the list until a connection is established.
- **sticky**—Specify that the router or switch first attempt to reconnect to the management server that it was last connected to. 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.

retry—Number of keepalive messages the router or switch sends without receiving a response from the client before the current SSH connection is disconnected. The default is three messages.

secret—(Optional) Router's or switch's public SSH host key. If added to the **outbound-ssh** statement, during the initialization of the outbound SSH service, the router or switch passes its public key to the management server. This is the recommended method of maintaining a current copy of the router's or switch's public key.

timeout—Length of time that the Junos server waits for data before sending a keep alive signal. The default is 15 seconds.

When reconnecting to a client, the router or switch attempts to reconnect to the client based on the **retry** and **timeout** values for each client listed.

address—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**—Outbound SSH port for the client. The default is port 22.
- **retry**—Number of times the router or switch attempts to establish an outbound SSH connection before giving up. The default is three tries.
- **timeout**—Length of time that the router or switch attempts to establish an outbound SSH connection before giving up. The default is fifteen seconds.

filename—(Optional) By default, the filename of the log file used to record the trace options is the name of the traced process (for example, **mib2d** or **snmpd**). Use this option to override the default value.

files—(Optional) 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 filename 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) 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 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**.

services—Services available for the session. Currently, NETCONF is the only service available.

world-readable | no-world-readable—(Optional) 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) Type of tracing operation to perform.

all—Log all events.

configuration—Log all events pertaining to the configuration of the router or switch.

connectivity—Log all events pertaining to the establishment of a connection between the client server and the router or switch.

no-remote-trace—(Optional) Disable remote tracing.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Outbound SSH Service on page 227
- System Management Configuration Statements on page 53

passive-learning

Syntax

passive-learning;

Hierarchy Level

[edit system arp]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure backup VRRP routers or switches to learn the ARP mappings (IP-to-MAC address) for hosts sending the requests.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 258

password (DHCP Local Server)

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 **dhcpv6 authentication**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication**],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication**],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6**],
[edit system services dhcp-local-server dhcpv6 **group** *group-name* **authentication**],
[edit system services dhcp-local-server **group** *group-name* **authentication**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Configure the password that is sent to the external AAA authentication server for subscriber authentication.

Options ***password-string***—Authentication password.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using External AAA Authentication Services with DHCP

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.

The remaining 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 Documentation

- Special Requirements for Junos OS Plain-Text Passwords on page 72
- **maximum-length on page 381**

path-mtu-discovery

Syntax (path-mtu-discovery | no-path-mtu-discovery);

Hierarchy Level [edit system **internet-options**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 enabled.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 256

peer

Syntax peer *address* <key *key-number*> <version *value*> <prefer>;

Hierarchy Level [edit system **ntp**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For NTP, configure the local router or switch to operate in symmetric active mode with the remote system at the specified address. In this mode, the local router or switch and the remote system can synchronize with each other. This configuration is useful in a network in which either the local router or switch 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the NTP Time Server and Time Services on page 132

permissions

Syntax permissions [*permissions*];

Hierarchy Level [edit system login class]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the login access privileges to be provided on the router or switch.

Options ***permissions***—Privilege type. For a list of permission flag types, see Table 7 on page 87.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Access Privilege Levels on page 92
- **user on page 464**

pic-console-authentication

Syntax

```
pic-console authentication {
  (encrypted-password "password" | plain-text-password);
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Set Console and Auxiliary Port Properties on page 234
- Configuring Password Authentication for Console Access to PICs on page 238

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches 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.

The remaining 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 Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

pool-match-order

Syntax

```
pool-match-order {
  external-authority;
  ip-address-first;
  option-82;
}
```

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 OS 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.

The remaining statements are explained separately.

Default

DHCP local server uses the **ip-address-first** method to determine which address pool to use.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use
- Extended DHCP Local Server Overview

port

Syntax port *port number*;

Hierarchy Level [edit system syslog host *hostname* | other-routing-engine| scc-master)],

Release Information Statement introduced in Junos OS Release 11.3.
Statement introduced in Junos OS Release 11.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Specify the port number for the remote syslog server.

Options *port number*—Port number of the remote syslog server.

Range: 0 through 65535

Default: 514

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- **syslog on page 439**
- **host on page 357**

port (HTTP/HTTPS)

Syntax port *port-number*;

Hierarchy Level [edit system services web-management]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the port on which the HTTP or HTTPS service is connected.

Options *port-number*—The TCP port number on which the specified service listens.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Management Access for the EX Series Switch (J-Web Procedure)
- *J-Web Interface User Guide*
- **http on page 359**
- **https on page 360**
- **web-management on page 469**

port (NETCONF Server)

Syntax port *port-number*;

Hierarchy Level [edit system services netconf]

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure the TCP port used for NETCONF-over-SSH connections.

NOTE:

- The configured port accepts only NETCONF-over-SSH connections. Regular SSH session requests for this port are rejected.
- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, you can specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

Options **port** ***port-number***—Port number on which to enable incoming NETCONF connections over SSH.

Default: **830** (as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*)

Range: **1** through **65535**

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *NETCONF XML Management Protocol Guide*
- Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 231

port (RADIUS Server)

Syntax port *port-number*;

Hierarchy Level [edit system radius-server *address*],
[edit system accounting destination radius server *address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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)

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication on page 103
- Configuring RADIUS Authentication

port (SRC Server)

Syntax port *port-number*;

Hierarchy Level [edit system services service-deployment servers *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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**

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Work with SRC Software on page 250

port (TACACS+ Server)

Syntax port *port-number*;

Hierarchy Level [edit system accounting destination tacplus server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring TACACS+ System Accounting on page 248

ports

Syntax

```
ports {
  auxiliary {
    disable;
    insecure;
    type terminal-type;
  }
  console {
    disable;
    insecure;
    log-out-on-disconnect;
    type terminal-type;
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the properties of the console and auxiliary ports. The ports are located on the router's craft interface.

See the switch's hardware documentation for port locations.

The remaining 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 Documentation

- Configuring the Junos OS to Set Console and Auxiliary Port Properties on page 234

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure which Junos OS processes are running on the router or switch.

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) Enable or disable a specified process.

failover (alternate-media | other-routing-engine)—(Optional) For routers or switches 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 or switch 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.

Values: **15**, **60**, or **180**

Default: **180** seconds (rounded up to 291 seconds by the Junos kernel)

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Disabling Junos OS Processes on page 240

protocol-version

Syntax protocol-version *version*;

Hierarchy Level [edit system services ssh]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify the secure shell (SSH) protocol version.

Default **[v1 v2]**

Options ***version***—SSH protocol version: **v1**, **u2**, or both

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the SSH Protocol Version on page 227

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the RADIUS accounting server.

Options ***server-address***—Address of the RADIUS accounting server.

The remaining 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 Documentation

- Configuring RADIUS System Accounting on page 246

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 OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options

nas-ip-address *ip-address*—IP address of the network access server (NAS) that requests user authentication.

password-protocol *mschap-v2*—Protocol MS-CHAPv2, used for password authentication and password changing.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring MS-CHAPv2 for Password-Change Support on page 104
- Configuring RADIUS Authentication

radius-server

Syntax

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

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication on page 103

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of connections attempts per protocol (either IPv6 or IPv4) on an access service.

Default **150** connections

Options **rate-limit** ***limit***—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).

Range: **1** through **250**

Default: **150**

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Number of times the router or switch 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication on page 103
- Configuring RADIUS System Accounting on page 246
- **timeout on page 447**

retry-options

Syntax

```
retry-options {
  backoff-threshold number;
  backoff-factor seconds;
  maximum-time seconds;
  minimum-time seconds;
  tries-before-disconnect number;
}
```

Hierarchy Level **[edit system login]**

Release Information Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
maximum-time option introduced in Junos OS Release 9.6.
maximum-time option introduced in Junos OS Release 9.6 for EX Series switches.

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

maximum-time *seconds*—Maximum length of time that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured **maximum-time**, the connection is closed.

Range: 20 through 300

Default: 120

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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 82
- **rate-limit on page 415**

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the authentication methods for the root-level user, whose username is **root**.

Options **encrypted-password "*password*"**— 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—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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Root Password on page 70
- **authentication on page 307**

root-login

Syntax root-login (allow | deny | deny-password);

Hierarchy Level [edit system services ssh]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Control user access through SSH.

Default Allow user access through SSH.

Options **allow**—Allow users to log in to the router or switch as root through SSH.

deny—Disable users from logging in to the router or switch as root through SSH.

deny-password—Allow users to log in to the router or switch as root through SSH when the authentication method (for example, RSA authentication) does not require a password.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Root Login Through SSH on page 226

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 OS 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.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

routing-instance-name (DHCP Local Server)

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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 authentication username-include**],
[edit system services dhcp-local-server **dhcpv6 authentication username-include**],
[edit system services dhcp-local-server dhcpv6 **group** *group-name* **authentication username-include**],
[edit system services dhcp-local-server **group** *group-name* **authentication username-include**]

Release Information

Statement introduced in Junos OS Release 9.1.

Description

Specify that the routing instance name be concatenated with the username during the subscriber authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services with DHCP

saved-core-context

Syntax (saved-core-context | no-saved-core-context);

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Saving Core Files from Junos OS Processes on page 242
- **saved-core-files on page 422**

saved-core-files

Syntax saved-core-files *number*;

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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 **10**

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Saving Core Files from Junos OS Processes on page 242
- **saved-core-context on page 422**

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the password to use with the RADIUS or TACACS+ server. The secret password used by the local router or switch must match that used by the server.

Options ***password***—Password to use; can include spaces included in quotation marks.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication on page 103
- Configuring TACACS+ Authentication on page 108
- Configuring TACACS+ System Accounting on page 248
- Configuring RADIUS System Accounting on page 246

server (NTP)

Syntax server *address* <key *key-number*> <version *value*> <prefer>;

Hierarchy Level [edit system ntp]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For NTP, configure the local router or switch to operate in client mode with the remote system at the specified ***address***. In this mode, the local router or switch can be synchronized with the remote system, but the remote system can never be synchronized with the local router or switch.

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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the NTP Time Server and Time Services on page 132

server (RADIUS Accounting)

Syntax

```
server {
  server-address {
    accounting-port port-number;
    retry number
    secret password;
    source-address address;
    timeout seconds;
  }
}
```

Hierarchy Level [edit system accounting destination radius]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure RADIUS logging.

The remaining 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 Documentation

- Configuring RADIUS System Accounting on page 246

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure TACACS+ logging.

The remaining 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 Documentation

- Configuring TACACS+ System Accounting on page 248

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services Routers and EX Series switches only. Configure a server identifier. The identifier 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*—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).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

servers

Syntax

servers *server-address* {
  port *port-number*;
}

Hierarchy Level [edit system services **service-deployment**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure an IPv4 address for the Session and Resource Control (SRC) server.

Options ***server-address***—The TCP port number.

Default: 3333

The remaining 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 Documentation

- Configuring the Junos OS to Work with SRC Software on page 250

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining 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 Documentation

- Configuring the Junos OS to Work with SRC Software on page 250

services

Syntax

```
services {
  dhcp { \* DHCP not supported on a DCF
    dhcp_services;
  }
  finger {
    connection-limit limit;
    rate-limit limit;
  }
  ftp {
    connection-limit limit;
    rate-limit limit;
  }
  service-deployment {
    servers address {
      port-number port-number;
    }
    source-address address;
  }
  ssh {
    connection-limit limit;
    protocol-version [v1 v2];
    rate-limit limit;
    root-login (allow | deny | deny-password);
  }
  telnet {
    connection-limit limit;
    rate-limit limit;
  }
  web-management {
    http {
      interfaces [ names ];
      port port;
    }
    https {
      interfaces [ names ];
      local-certificate name;
      port port;
    }
    session {
      idle-timeout [ minutes ];
      session-limit [ limit ];
    }
  }
  xnm-clear-text {
    connection-limit limit;
    rate-limit limit;
  }
  xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
  }
```


}

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, finger, rlogin, SSH, telnet, Web management, Junos XML protocol clear-text, Junos XML protocol SSL, and network utilities or enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining 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 Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189
- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190
- Configuring the Junos OS to Work with SRC Software on page 250

session

Syntax

```
session {
  idle-timeout minutes;
  session-limit session-limit;
}
```

Hierarchy Level [edit **system services web-management**]

Release Information Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *J-Web Interface User Guide*

single-connection

Syntax single-connection;

Hierarchy Level [edit system accounting destination tacplus-server *server-address*]
[edit system **tacplus-server** *server-address*],

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring TACACS+ Authentication on page 108
- Configuring TACACS+ System Accounting on page 248

size

Syntax size *size*;

Hierarchy Level [edit system syslog archive],
[edit system syslog file *filename* archive]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum amount of data that the Junos OS 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: 1 MB for MX Series routers and the QFX Series

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 156
- *Junos OS System Log Messages Reference*
- **files on page 350**

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 or switch 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 router or TX Matrix Plus router in a routing matrix based on a TX Matrix router or TX Matrix Plus router.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 105
- Specifying a Source Address for an NTP Server on page 129
- Specifying an Alternative Source Address for System Log Messages on page 151

source-address (SRC Software)

Syntax source-address *source-address*;

Hierarchy Level [edit system services service-deployment]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Enable Junos OS to work with the Session and Resource Control (SRC) software.

Options ***source-address***— 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Work with SRC Software on page 250

source-port

Syntax source-port upper-limit <*upper-limit*>;

Hierarchy Level [edit system **internet-options**]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Extend the Default Port Address Range on page 257

source-quench

Syntax
(source-quench | no-source-quench);

Hierarchy Level
[edit system **internet-options**]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure how the Junos OS handles Internet Control Message Protocol (ICMP) source quench messages:

- **source-quench**—The Junos OS ignores ICMP source quench messages.
- **no-source-quench**—The Junos OS does not ignore ICMP source quench messages.

Default
The Junos OS does not ignore ICMP source quench messages.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS to Ignore ICMP Source Quench Messages on page 256

ssh

Syntax
```
ssh {
  connection-limit limit;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
}
```

Hierarchy Level
[edit system services]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Allow SSH requests from remote systems to the local router or switch.

The remaining 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 Documentation
- Configuring SSH Service for Remote Access to the Router or Switch on page 226

static-binding

Syntax

```
static-binding mac-address {
  client-identifier (ascii client-id | hexadecimal client-id);
  fixed-address {
    address;
  }
  host-name client-hostname;
}
```

Hierarchy Level [edit system services **dhcp**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For J Series Services routers and EX Series switches 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-name *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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

static-host-mapping

Syntax

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

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS 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***—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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Hostname of the Router or Switch on page 62

structured-data

Syntax

```
structured-data {
  brief;
}
```

Hierarchy Level [edit system syslog file *filename*]

Release Information Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Write system log messages to the log file in structured-data format, which complies with Internet draft draft-ietf-syslog-protocol-23, *The syslog Protocol* (http://tools.ietf.org/html/draft-ietf-syslog-protocol-23).

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).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Logging Messages in Structured-Data Format on page 148
- *Junos OS System Log Messages Reference*
- **explicit-priority on page 347**
- **time-format on page 446**

syslog

Syntax

```
syslog {
  archive {
    files number;
    size maximum-file-size;
    start-time "YYYY-MM-DD.hh:mm";
    transfer-interval minutes;
    (world-readable | no-world-readable);
  }
  console {
    facility severity;
  }
  file filename {
    facility severity;
    explicit-priority;
    match "regular-expression";
    archive {
      files number;
      size maximum-file-size;
      start-time "YYYY-MM-DD.hh:mm";
      transfer-interval minutes;
      (world-readable | no-world-readable);
    }
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    port port number;
  }
  source-address source-address;
  time-format (millisecond | year | year millisecond);
  user (username | *) {
    facility severity;
    match "regular-expression";
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the types of system log messages to log to files, a remote destination, user terminals, or the system console.

The remaining 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 Documentation
- Junos OS System Log Configuration Overview on page 139
- *Junos OS System Log Messages Reference*
- Overview of Single-Chassis System Logging Configuration

system

Syntax system { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure system management properties.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- System Management Configuration Statements on page 53

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring TACACS+ System Accounting on page 248

tacplus-options

Syntax

```
tacplus-options {
  (exclude-cmd-attribute | no-cmd-attribute-value);
  service-name service-name;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for QFX Series.
no-cmd-attribute-value and **exclude-cmd-attribute** options introduced in Junos OS Release 9.3.
no-cmd-attribute-value and **exclude-cmd-attribute** options introduced in Junos OS Release 9.3 for EX Series switches.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 109
- Configuring TACACS+ Server Accounting on page 249
- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 116
- Configuring TACACS+ Authentication
- Configuring TACACS+ System Accounting

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the TACACS+ server.

Options ***server-address***—Address of the TACACS+ authentication server.

The remaining 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 Documentation

- Configuring TACACS+ Authentication on page 108

tcp-drop-synfin-set

Syntax tcp-drop-synfin-set;

Hierarchy Level [edit system internet-options]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the router or switch to drop packets that have both the SYN and FIN bits set.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set on page 256

tcp-mss

Syntax tcp-mss *mss-value*;

Hierarchy Level [edit system internet-options]

Release Information Statement introduced in Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring TCP MSS on J Series Services Routers on page 253

telnet

Syntax

```
telnet {
  connection-limit limit;
  rate-limit limit;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Provide Telnet connections from remote systems to the local router or switch.

The remaining 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 Documentation

- Configuring Telnet Service for Remote Access to a Router or Switch on page 232

time-format

Syntax time-format (year | millisecond | year millisecond);

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Including the Year or Millisecond in Timestamps on page 161
- *Junos OS System Log Messages Reference*
- **structured-data on page 438**

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the amount of time that the local router or switch 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication on page 103
- Configuring TACACS+ Authentication on page 108
- **retry on page 416**

time-zone

Syntax time-zone (GMT *hour-offset* | *time-zone*);

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
GMT ***hour-offset*** option added in Junos OS Release 7.4.

Description Set the local time zone. To have the time zone change take effect for all processes running on the router or switch, you must reboot the router or switch.

Default UTC

Options **GMT** ***hour-offset***—Set the time zone relative to UTC time.

Range: –14 through +12

Default: 0

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

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Modifying the Default Time Zone for a Router or Switch Running Junos OS on page 127
- System Management Configuration Statements on page 53

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 OS Release 9.0.
option-name option introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure tracing options.

Options

file *filename*—Name of the file that receives the output of the tracing operation. Enclose the name in 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.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

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.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

traceoptions (DHCP Local Server)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximu-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

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 OS Release 9.0.

Description

Define global tracing operations for DHCP local server processes. You use the **trace** statement to configure interface-specific tracing.

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 to create before overwriting the oldest one. 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: 3 files

flag ***flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. See Configuring the Extended DHCP Tracing Flags for a list of the flags that you can include.

match ***regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Allow only the user **root** and users who have the Junos **maintenance** permission to access the trace files.

size ***maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable all users to access the trace files.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing Extended DHCP Operations
- Configuring the Extended DHCP Log Filename
- Configuring the Number and Size of Extended DHCP Log Files
- Configuring Access to the Extended DHCP Log File
- Configuring a Regular Expression for Extended DHCP Lines to Be Logged
- Configuring the Extended DHCP Tracing Flags

traceoptions (DHCP Server)

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 OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Define tracing operations for DHCP processes for J Series Services Routers and EX Series switches.

Options **file *filename***—Name of the file that receives the output of the tracing operation. Enclose the name in 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
- **match *regex***— Refine the output to include lines that contain the regular expression.
- **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

no-world-readable—(Optional) Disable unrestricted file access.

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.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Tracing Operations for DHCP Processes on page 206
- System Management Configuration Statements on page 53

traceoptions (SBC Configuration Process)

Syntax

```
traceoptions {
  file filename <files number> <match regex> <size size>
    <world-readable | no-world-readable>;
  flag flag;
}
```

Hierarchy Level [edit system processes sbc-configuration-process]

Release Information Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.

Description Configure trace options for the session border controller (SBC) process of the border signaling gateway (BSG).

Options **file *filename***—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**. You can include the following file 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 must also specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000
Default: 3 files

- **match *regex***—(Optional) Refine the output to include lines that contain the regular expression.
- **no-world-readable**—(Optional) Disable unrestricted file access.
- **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.

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-level***—Trace all SBC process operations.
- **common** ***trace-level***—Trace common events.
- **configuration** ***trace-level***—Trace configuration events.
- **device-monitor** ***trace-level***—Trace device monitor events.
- **ipc** ***trace-level***—Trace IPC events.
- **memory—pool** ***trace-level***—Trace memory pool events.
- ***trace-level***—Trace level options are related to the severity of the event being traced. When you choose a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels as the ***trace-level***:
  - **debug**—Log all code flow of control.
  - **error**—Log failures with a short-term effect.
  - **info**—Log summary for normal operations, such as the policy decisions made for a call.
  - **trace**—Log program trace START and EXIT macros.
  - **warning**—Log failure recovery events or failure of an external entity.
- **ui** ***trace-level***—Trace user interface operations.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- See “Troubleshooting the IMSG” in the *Junos Multiplay Solutions Guide*
- System Management Configuration Statements on page 53

tracing

Syntax

```
tracing {
  destination-override syslog host ip-address;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure the router to enable remote tracing to a specified host 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Junos OS Tracing and Logging Operations on page 49
- **destination-override on page 334**
- **no-remote-trace on page 389**

transfer-interval (Configuration)

Syntax transfer-interval *interval*;

Hierarchy Level [edit system archival configuration]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the router or switch 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Transfer Interval for Periodic Transfer of the Active Configuration to an Archive Site on page 244
- **archive on page 301**
- **configuration on page 323**
- **transfer-on-commit on page 462**

transfer-on-commit

Syntax transfer-on-commit;

Hierarchy Level [edit system archival configuration]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the router or switch 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 OS 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*” .

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Transfer of the Current Active Configuration When a Configuration Is Committed on page 244
- **archive on page 301**
- **configuration on page 323**
- **transfer-interval on page 461**

trusted-key

Syntax trusted-key [*key-numbers*];

Hierarchy Level [edit system **ntp**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For NTP, configure the keys you are allowed to use when you configure the local router or switch 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring NTP Authentication Keys on page 134
- **authentication-key on page 308**
- **broadcast on page 316**
- **peer on page 400**
- **server on page 424**

uid

Syntax uid *uid-value*;

Hierarchy Level [edit system login **user**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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 or switch.

Range: **100** through **64000**

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Junos OS User Accounts on page 81

use-imported-time-zones

Syntax use-imported-time-zones;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure a custom time zone from a locally generated time-zone database.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Setting a Custom Time Zone on Routers or Switches Running Junos OS on page 136

user (Access)

Syntax

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

Hierarchy Level [edit system login]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure access permission for individual users.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Junos OS User Accounts on page 81
- class on page 319

user (System Logging)

Syntax

```
user (username | *) {
  facility severity;
  match "regular-expression";
}
```

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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 15 on page 146.

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 16 on page 147.

username—Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Directing System Log Messages to a User Terminal on page 149
- Junos OS System Logging Facilities and Message Severity Levels on page 146
- *Junos OS System Log Messages Reference*

username-include (DHCP Local Server)

Syntax

username-include {
  circuit-type;
  client-id;
  delimiter *delimiter-character*;
  domain-name *domain-name-string*;
  logical-system-name;
  mac-address;
  option-60;
  option-82 <circuit-id> <remote-id>;
  relay-agent-interface-id;
  relay-agent-remote-id;
  relay-agent-subscriber-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 **dhcpv6 authentication**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication**],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication**],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication**],
[edit system services dhcp-local-server dhcpv6 **group** *group-name* **authentication**],
[edit system services dhcp-local-server **group** *group-name* **authentication**]

Release Information Statement introduced in Junos OS 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. The **option-60** and **option-82** statements are not supported in the DHCPv6 hierarchy levels. The client-id, relay-agent-interface-id, relay-agent-remote-id and relay-agent-subscriber-id statements are supported in the DHCPv6 hierarchy levels only.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services with DHCP
- Creating Unique Usernames for DHCP Clients

user-prefix (DHCP Local Server)

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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 authentication username-include**],
[edit system services dhcp-local-server **dhcpv6 authentication username-include**],
[edit system services dhcp-local-server dhcpv6 **group** *group-name* **authentication username-include**],
[edit system services dhcp-local-server **group** *group-name* **authentication username-include**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify the user prefix that is concatenated with the username during the subscriber authentication process.

Options ***user-prefix-string***—User prefix string.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using External AAA Authentication Services with DHCP

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure settings for HTTP or HTTPS access. HTTP access allows management of the router or switch using the browser-based J-Web graphical user interface. HTTPS access allows secure management of the router or switch using the J-Web interface. With HTTPS access, communication between the router or switch Web server and your browser is encrypted.

The remaining 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 Documentation
- Configuring Management Access for the EX Series Switch (J-Web Procedure)
- *J-Web Interface User Guide*
- **http on page 359**
- **https on page 360**
- **port on page 405**

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

For J Series Services Routers and EX Series switches 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.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Router, Switch, or Interface to Act as a DHCP Server on J Series Services Routers and EX Series Ethernet Switches on page 190

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 156
- *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 OS Release 7.4.

Description Allow Junos XML protocol clear-text requests from remote systems to the local router.

The remaining 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 Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189

xnm-ssl

Syntax

xnm-ssl {
  connection-limit *limit*;
  rate-limit *limit*;
}

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.

Description Allow Junos XML protocol SSL requests from remote systems to the local router.

The remaining 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 Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189

PART 3

Access

CHAPTER 14

Configuring Access

This chapter includes the following topics:

- RADIUS Attributes for L2TP on page 506
- Example: Configuring RADIUS Authentication for L2TP on page 510
- Configuring the RADIUS Disconnect Server for L2TP on page 511
- Configuring RADIUS Authentication for an L2TP Client and Profile on page 512
- Example: Configuring RADIUS Authentication for an L2TP Profile on page 513
- Configuring an IKE Access Profile on page 513

Access Configuration Statements

To configure access, include the following statements at the **[edit access]** hierarchy level:

```
[edit access]
address-assignment {
  neighbor-discovery-router-advertisement;
  pool pool-name {
    family inet {
        dhcp-attributes {
          [protocol-specific-attributes];
        }
        host hostname {
          hardware-address mac-address;
          ip-address ip-address;
        }
      network address-or-prefix </subnet-mask>;
        range name {
        high upper-limit;
        low lower-limit;
        prefix-length prefix-length;
      }
    }
  }
}
address-pool pool-name {
  address address-or-prefix;
  address-range low <lower-limit> high <upper-limit>;
}
domain {
  delimiter;
  map;
  parse-direction;
};
group-profile profile-name {
  l2tp {
    interface-id interface-id;
    lcp-renegotiation;
    local-chap;
    maximum-sessions-per-tunnel number;
    multilink {
      drop-timeout milliseconds;
      fragment-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;
        coa-immediate-update;
        immediate-update;
        order [ accounting-method ];
        statistics (time | volume-time);
        update-interval minutes;
    }
    accounting-order radius;
    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;
            ipsec-policy ipsec-policy;
            interface-id interface-id;
        }
        l2tp {
            interface-id interface-id;
            lcp-renegotiation;
            local-chap;
            maximum-sessions-per-tunnel number;
            multilink {
                drop-timeout milliseconds;
                fragment-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);
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    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;
    }
    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;
}
```

Related Documentation

- Configuring the PPP Authentication Protocol on page 480
- Example: Configuring PPP CHAP on page 480
- Configuring the PPP Authentication Protocol on page 480
- Example: Configuring CHAP Authentication with RADIUS on page 481
- Configuring L2TP for Enabling PPP Tunneling Within a Network on page 484
- Defining the Minimum L2TP Configuration on page 485
- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 486
- Configuring the Group Profile for Defining L2TP Attributes on page 487

Configuring the PPP Authentication Protocol

The Point-to-Point Protocol (PPP) is an encapsulation protocol for transporting IP traffic across point-to-point links. 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.

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.

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.

Related Documentation

- Example: Configuring PPP CHAP on page 480
- Example: Configuring CHAP Authentication with RADIUS on page 481

Example: Configuring PPP CHAP

The following example shows how to 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";
          }
        }
      }
    }
```

Related Documentation

- Configuring the PPP Authentication Protocol on page 480

Example: Configuring CHAP Authentication with RADIUS

You can send RADIUS messages through a routing instance to customer RADIUS servers in a private network. To configure the routing instance to send packets to a RADIUS server, 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 about RADIUS authentication, see “Configuring RADIUS Authentication” on page 103.

```
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).

Related Documentation

- Configuring the Authentication Order on page 491
- Example: Configuring PPP CHAP on page 480
- Configuring the PPP Authentication Protocol on page 480

Configuring L2TP for Enabling PPP Tunneling Within a Network

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 Point-to-Point Protocol (PPP) to be tunneled within a network.

NOTE: For information about how to configure L2TP service, see the *Junos OS Services Interfaces Configuration Guide* and the *Junos OS 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;
            routing-instance routing-instance-name;
            secret password;
            source-address source-address;
            timeout seconds;
        }
    }
```

Related Documentation

- Defining the Minimum L2TP Configuration on page 485
- Configuring RADIUS Authentication for L2TP on page 505

Defining the Minimum L2TP Configuration

To define the minimum configuration for the Layer 2 Tunneling Protocol (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.

Related Documentation

- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 486

Configuring the Address Pool for L2TP Network Server IP Address Allocation

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 PPP Properties for a Client-Specific Profile" on page 499.

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.

Related Documentation

- Configuring the Group Profile for Defining L2TP Attributes on page 487
- Defining the Minimum L2TP Configuration on page 485

Configuring the Group Profile for Defining L2TP Attributes

Optionally, you can configure the group profile to define the Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol (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 501.

Tasks for configuring the group profile are:

1. Configuring L2TP for a Group Profile on page 488
2. Configuring the PPP Attributes for a Group Profile on page 488

Configuring L2TP for a Group Profile

To configure the Layer 2 Tunneling Protocol (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.

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 OS 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 Point-to-Point Protocol (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.

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.

seconds (in the **keepalive** statement) is the time period that must elapse before the Junos OS checks the status of the PPP session by sending an echo request to the peer. For each session, Junos OS 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 message 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

The following example shows how to 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;
  }
}
```

Related Documentation

- Configuring the Group Profile for Defining L2TP Attributes on page 487
- Defining the Minimum L2TP Configuration on page 485
- Referencing the Group Profile from the L2TP Profile on page 495

Configuring Access Profiles for L2TP or PPP Parameters

To validate Layer 2 Tunneling Protocol (L2TP) connections and session requests, you set up access profiles by configuring the profile statement at the **[edit access]** hierarchy level. You can configure multiple profiles. You can also configure multiple clients for each profile.

Tasks for configuring the access profile are:

1. Configuring the Access Profile on page 490
2. Configuring the L2TP Properties for a Profile on page 490
3. Configuring the PPP Properties for a Profile on page 491
4. Configuring the Authentication Order on page 491
5. Configuring the Accounting Order on page 492

Configuring the Access 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 501.

When you configure a profile, you can only configure either L2TP or PPP parameters. You cannot configure both at the same time.

Configuring the L2TP Properties for a Profile

To configure the Layer 2 Tunneling Protocol (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;
```

Configuring the PPP Properties for a Profile

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.

Configuring the Authentication Order

You can configure the order in which the Junos OS 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 505.

If you do not include the **authentication-order** statement, clients are verified by means of **password** authentication.

Configuring the Accounting Order

You can configure RADIUS accounting for an L2TP profile.

With RADIUS accounting enabled, Juniper Networks routers or switches, 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.

Configuring the L2TP 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.

Related Documentation

• Example: Defining the Default Tunnel Client on page 493

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.

Related Documentation

• Configuring the L2TP Client on page 493
• Example: Defining the User Group Profile on page 493

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;
}
```

Related Documentation

- Applying a Configured PPP Group Profile to a Tunnel on page 501.

Configuring the CHAP Secret for an L2TP Profile

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.

NOTE: When you configure PPP properties for a Layer 2 Tunneling Protocol (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.

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.

Related Documentation

- Example: Configuring L2TP PPP CHAP on page 495

Example: Configuring L2TP 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
  }
}
```

Related Documentation

- Configuring the CHAP Secret for an L2TP Profile on page 494

Referencing the Group Profile from the L2TP 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.

Related Documentation

- Example: Defining the User Group Profile on page 493
- Configuring Access Profiles for L2TP or PPP Parameters on page 490
- Configuring L2TP Properties for a Client-Specific Profile on page 495

Configuring L2TP Properties for a Client-Specific Profile

To define L2TP properties for a client-specific 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 configure either L2TP or PPP parameters, but not both at the same time.

```
[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;
    fragment-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.

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-negotiation** 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 OS 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 OS 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 **fragment-threshold** statement). If a packet exceeds the fragmentation threshold, the Junos OS fragments it into two or more multilink fragments.

Related Documentation

- Configuring PPP Properties for a Client-Specific Profile on page 499
- Example: PPP MP for L2TP on page 497
- Example: L2TP Multilink PPP Support on Shared Interfaces on page 497

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;
      }
    }
  }
}
```

Related Documentation

- Referencing the Group Profile from the L2TP Profile on page 495
- Example: L2TP Multilink PPP Support on Shared Interfaces on page 497

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 "$9$Vyb4ZHkPQ39mf9pORlexNdbgoZUjqP5"; # 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;
            }
          }
        }
      }
```

Related Documentation

- Referencing the Group Profile from the L2TP Profile on page 495

Configuring the PAP 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 for an L2TP Profile” on page 494.

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.

Related Documentation

- Example: Configuring PAP for an L2TP Profile on page 499

Example: Configuring PAP for an L2TP Profile

The following examples shows you how to configure the password authentication protocol 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;
    }
  }
}
```

Related Documentation

- Configuring the PAP Password for an L2TP Profile on page 498

Configuring PPP Properties for a Client-Specific 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.

NOTE: 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*;
keepalive-retries *number-of-retries*;
primary-dns *primary-dns*;
primary-wins *primary-wins*;
secondary-dns *secondary-dns*;
secondary-wins *secondary-wins*;

NOTE: When you configure a profile, you can configure either L2TP or PPP parameters, but not both at the same time.

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.

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.

keepalive *seconds* is the time period that must elapse before the Junos OS checks the status of the PPP session by sending an echo request to the peer. For each session, Junos OS sends a maximum of ten 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 can configure this to be a value in the range from 0 through 32,767 seconds.

keepalive-retries *number-of-retries* is the number of retry attempts for checking the keepalive status of a Point-to-Point (PPP) protocol session. Configuring a lower number of retries helps reduce the detection time for PPP client session failures or timeouts if you have configured a **keepalive *seconds*** value. By default, the number of retries is set to 10 times. You can configure this to be a value in the range from 3 through 32,767 times.

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.

Related Documentation

- Configuring L2TP Properties for a Client-Specific Profile on page 495

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 OS 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.

Related Documentation

- Example: Applying a User Group Profile on the M7i or M10i Router on page 501
- Example: Defining the User Group Profile on page 493

Example: Applying a User Group Profile on the M7i or M10i Router

The following example shows how to 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
    }
  }
```

Related Documentation

- Applying a Configured PPP Group Profile to a Tunnel on page 501

Example: Configuring the Access Profile

The following example shows you how to configure the access 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;
    }
  }
```

Related Documentation

- Configuring Access Profiles for L2TP or PPP Parameters on page 490

Example: Configuring L2TP

The following example shows how to 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 is CHAP.
    }
    group-profile westcoast_tunnel;
  }
  client production {
    l2tp {
      shared-secret "$9$R2QErv8X-goGylVwg4jiTz36/t0BEleWFnRh
      rlXxbs2aJDHqf3nCP5"; # SECRET-DATA
      ppp-authentication chap;
    }
    group-profile westcoast_tunnel;
  }
}
profile westcoast_bldg_2_tunnel {
  client black {
```



```
                l2tp {
                    shared-secret "$9$R2QErv8X-goGylVwg4jiTz36/t0BEleWFnRh
                    rlXxbs2aJDHqf3nCP5";
                    # SECRET-DATA
                    ppp-authentication pap;
                }
                group-profile westcoast_tunnel;
            }
        }
    }
```

Related Documentation

- Configuring L2TP for Enabling PPP Tunneling Within a Network on page 484

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. If the maximum number of retries is reached, the radius server is considered dead for 5 minutes (300 seconds).

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 511.

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.**

Related Documentation

- RADIUS Attributes for L2TP on page 506
- Configuring L2TP for Enabling PPP Tunneling Within a Network on page 484
- Configuring the RADIUS Disconnect Server for L2TP on page 511

RADIUS Attributes for L2TP

The Junos OS 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 507 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
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 507 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

Table 34: Supported IETF RADIUS Attributes for L2TP *(continued)*

Attribute Name	Standard Number	Value
Calling-Station-ID	31	String
CHAP-Challenge	60	String
NAS-Port-Type	61	Integer
Framed-Pool	88	Integer

Table 35 on page 508 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

Table 35: Supported RADIUS Accounting Start Attributes for L2TP *(continued)*

Attribute Name	Standard Number	Value
Tunnel-Server-Auth-ID	91	String

Table 36 on page 509 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

Table 36: Supported RADIUS Accounting Stop Attributes for L2TP *(continued)*

Attribute Name	Standard Number	Value
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

Related Documentation

- Example: Configuring RADIUS Authentication for L2TP on page 510

Example: Configuring RADIUS Authentication for L2TP

The following example shows how to configure 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 "$9$rtkl87ws4ZDkgokPT3tpEcylWL7-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
}
```

Related Documentation

- Configuring RADIUS Authentication for L2TP on page 505

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 OS 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 or switch 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 505.

The following example shows the statements to be included at the **[edit access]** hierarchy level to configure the RADIUS disconnect server:

```
[edit access]
radius-disconnect-port 1700;
radius-disconnect {
  192.168.64.153 secret "$9$rtkl87ws4ZDkgokPT3tpEcylWL7-VY4a";
```

```
    # SECRET-DATA
    192.168.64.162 secret "$9$rtkl87ws4ZDkgokPT3tpEcylWL7-VY4a";
    # SECRET-DATA
}
```

Related Documentation

- Configuring RADIUS Authentication for L2TP on page 505

Configuring RADIUS Authentication for an L2TP Client and Profile

On an M10i or M7i router, 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 router, 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.

Related Documentation

- Example: Configuring RADIUS Authentication for an L2TP Profile on page 513

Example: Configuring RADIUS Authentication for an L2TP Profile

The following example shows statements to be included at the **[edit access]** hierarchy level to 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;
}
```

Related Documentation

- Configuring RADIUS Authentication for an L2TP Client and Profile on page 512

Configuring an IKE Access Profile

An Internet Key Exchange (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. 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.

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;
        ipsec-policy ipsec-policy;
      }
    }
  }
```

For dynamic peers, the Junos OS 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 preshared 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.
- **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.
- **ipsec-policy**—Name of the IPsec policy that defines the IPsec policy information for the session. You define the IPsec policy at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level. If no policy is set, any policy proposed by the dynamic peer is accepted.

Related Documentation

- Configuring Access Profiles for L2TP or PPP Parameters on page 490

CHAPTER 15

Summary of Access Configuration Statements

The following sections explain each of the access configuration statements. The statements are organized alphabetically.

accounting (Access Profile)

Syntax

```
accounting {
  accounting-stop-on-access-deny;
  accounting-stop-on-failure;
  coa-immediate-update;
  immediate-update;
  order [ accounting-method ];
  statistics (time | volume-time);
  update-interval minutes;
}
```

Hierarchy Level [edit access **profile** *profile-name*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Per-Subscriber Session Accounting

accounting-order

Syntax accounting-order radius;

Hierarchy Level [edit access **profile** *profile-name*]

Release Information Statement introduced in Junos OS Release 8.0.

Description Enable RADIUS accounting for an L2TP profile.

Options **radius**—Use the RADIUS accounting method.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Accounting Order on page 492

accounting-port

Syntax accounting-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 OS Release 7.4.

Description Configure the port number on which to contact the accounting server.

Options ***port-number***—Port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring RADIUS Authentication for L2TP on page 505

accounting-server

Syntax accounting-server [*ip-address*];

Hierarchy Level [edit access profile *profile-name* **radius**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS accounting servers used for accounting for DHCP, L2TP, and PPP clients.

Options ***ip-address***—IP version 4 (IPv4) address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access

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 OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the format the router or switch uses to identify the accounting session.

Default **decimal**

Options **decimal**—Use the decimal format.

description—Use the generic format, in the form: **jnpr** ***interface-specifier*:*subscriber-session-id***.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access
- Configuring Authentication and Accounting Parameters for Subscriber Access

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 OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting to send an Acct-Stop message when the AAA server refuses a client request for access.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access

accounting-stop-on-failure

Syntax accounting-stop-on-failure;

Hierarchy Level [edit access profile *profile-name* **accounting**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access

address

Syntax address *address-or-prefix*;

Hierarchy Level [edit access **address-pool** *pool-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the IP address or prefix value for clients.

Options ***address-or-prefix***—An address or prefix value.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 486

address-assignment (Address-Assignment Pools)

Syntax

```
address-assignment {
  abatedUtilization percentage;
  abatedUtilization-v6 percentage;
  highUtilization percentage;
  highUtilization-v6 percentage;
  neighbor-discovery-router-advertisement ndra-pool-name;
  pool pool-name {
    family family {
      dhcp-attributes {
        protocol-specific attributes;
      }
      host hostname {
        hardware-address mac-address;
        ip-address ip-address;
      }
      network ip-prefix/<prefix-length>;
      prefix ipv6-prefix;
      range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length prefix-length;
      }
    }
    link pool-name;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Allocate IP addresses for clients.

Options ***pool-name***—Name assigned to an address pool.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 486

address-range

Syntax address-range <low *lower-limit*> <high *upper-limit*>;

Hierarchy Level [edit access **address-pool** *pool-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the address range.

Options

- **high *upper-limit***—Upper limit of an address range.
- **low *lower-limit***—Lower limit of an address range.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Address Pool for L2TP Network Server IP Address Allocation on page 486

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* ike]

Release Information Statement introduced in Junos OS Release 7.4.

Description Specify the network address of the local and remote peer associated with an IKE access profile.

Options **local *local-proxy-address***—Network address of the local peer.

Default: 0.0.0.0

remote *remote-proxy-address*—Network address of the remote peer.

Default: 0.0.0.0

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IKE Access Profile on page 513

attributes

Syntax

```
attributes {
  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 ];
  }
  ignore {
    framed-ip-netmask;
    input-filter;
    logical-system-routing-instance;
    output-filter;
  }
}
```

Hierarchy Level [edit access profile *profile-name* **radius**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Specify how the router or switch processes RADIUS attributes.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring How RADIUS Attributes Are Used for Subscriber Access

authentication-order

Syntax authentication-order [*authentication-methods*];

Hierarchy Level [edit access **profile** *profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, the software tries the authentication methods in order, from first to last.

Default **password**

Options *authentication-methods*

- **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.

NOTE: For subscriber access management, you must always specify the **radius** method. Subscriber access management does not support the **password** option (the default), and authentication fails when no method is specified.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring CHAP Authentication with RADIUS on page 481
- Specifying the Authentication and Accounting Methods for Subscriber Access
- Configuring Access Profiles for L2TP or PPP Parameters on page 490

authentication-server

Syntax authentication-server [*ip-address*];

Hierarchy Level [edit access **profile** *profile-name* **radius**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.

Options ***ip-address***—IPv4 address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access

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 OS 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***—Location of the boot file on the boot server. The filename can include a pathname.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools
- **boot-server on page 526**

boot-server

Syntax boot-server (*address* | *hostname*);

Hierarchy Level [edit access address-assignment pool *pool-name* family inet **dhcp-attributes**]

Release Information Statement introduced in Junos OS 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***—IPv4 address of a boot server.

hostname—Fully qualified hostname of a boot server.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Address-Assignment Pools
- **boot-file on page 525**

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 OS Release 8.3.

Description Configure the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping on the IQ2 PIC.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

chap-secret

Syntax chap-secret *chap-secret*;

Hierarchy Level [edit access profile *profile-name* client *client-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the CHAP secret key associated with a peer.

Options ***chap-secret***—The secret key associated with a peer.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the CHAP Secret for an L2TP Profile on page 494

circuit-id (Address-Assignment Pools)

Syntax circuit-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 OS Release 9.0.

Description Configure the address-assignment pool named-range to use for a particular option 82 Agent Circuit ID value.

Options ***value***—String for the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) in DHCP packets.

range *named-range*—Name of the address-assignment pool range to use.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Address-Assignment Pools

circuit-type (DHCP Local Server)

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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 **dhcpv6 authentication username-include**],
[edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name* **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 authentication username-include**],
[edit system services dhcp-local-server **dhcpv6 authentication username-include**],
[edit system services dhcp-local-server dhcpv6 **group** *group-name* **authentication username-include**],
[edit system services dhcp-local-server **group** *group-name* **authentication username-include**]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify that the circuit type is concatenated with the username during the subscriber authentication process.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Using External AAA Authentication Services with DHCP

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;
      fragment-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 OS Release 7.4.

Description Configure the peer identity.

Options ***client-name***—A peer identity.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the L2TP Client on page 493
- Configuring Access Profiles for L2TP or PPP Parameters on page 490

client-authentication-algorithm

Syntax client-authentication-algorithm (direct | round-robin);

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure the access method the router uses to access RADIUS authentication servers.

Default direct

Options **direct**—Use the direct method.

round-robin—Use the round-robin method.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access
- Configuring RADIUS Server Options for Subscriber Access

dhcp-attributes (Address-Assignment Pools)

Syntax

```
dhcp-attributes {
  boot-file filename;
  boot-server (address | hostname);
  dns-server [ ipv6-address ];
  domain-name domain-name;
  grace-period seconds;
  maximum-lease-time seconds;
  name-server [ server-list ];
  netbios-node-type node-type;
  option {
    [ (id-number option-type option-value)
    (id-number array option-type option-value) ];
  }
  option-match {
    option-82 {
      circuit-id value range named-range;
      remote-id value range named-range;
    }
  }
  router [ router-address ];
  server-identifier ip4-address;
  sip-server-address [ ipv6-address ];
  sip-server-domain-name domain-name;
  tftp-server address;
  wins-server [ servers ];
}
```

Hierarchy Level [edit access address-assignment **pool** *pool-name* family *family*]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure address pools that can be used by different client applications.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools
- Configuring DHCP Client-Specific Attributes

domain-name (Address-Assignment Pools)

Syntax domain-name *domain-name*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet **dhcp-attributes**]

Release Information Statement introduced in Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Address-Assignment Pools

drop-timeout

Syntax drop-timeout *milliseconds*;

Hierarchy Level [edit access **profile** *profile-name* **client** *client-name* **l2tp multilink**]

Release Information Statement introduced before Junos OS 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 OS 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.)

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring L2TP Properties for a Client-Specific Profile on page 495

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

ethernet-port-type-virtual

Syntax ethernet-port-type-virtual;

Hierarchy Level [edit access profile *profile-name* radius **options**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of **ethernet** in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of **virtual**.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access

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 ];
  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-filter [ 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 OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the router or switch 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 or switch 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.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access

fragment-threshold

Syntax fragment-threshold *bytes*;

Hierarchy Level [edit access **profile** *profile-name* **client** *client-name* **l2tp multilink**]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the fragmentation threshold for a multilink bundle.

Options *bytes*—The maximum number of bytes in a packet. If a packet exceeds the fragmentation threshold, the Junos OS fragments it into two or more multilink fragments.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP Properties for a Client-Specific Profile on page 495
- **multilink on page 551**

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 OS Release 7.4.

Description Specify a framed IP address.

Options *address*—The IP version 4 (IPv4) prefix.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring PPP Properties for a Client-Specific Profile on page 499

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 OS Release 7.4.

Description Configure the address pool.

Options *framed-pool*—References a configured address pool.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

grace-period

Syntax grace-period *seconds*;

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6) dhcp-attributes]

Release Information Statement introduced in Junos OS 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)

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

group-profile (Associating with Client)

Syntax group-profile *profile-name*;

Hierarchy Level [edit access profile *profile-name* **client** *client-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Associate a group profile with a client.

Options ***profile-name***—Name assigned to the group profile.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Referencing the Group Profile from the L2TP Profile on page 495

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 OS Release 7.4.

Description Configure the group profile.

Options ***profile-name***—Name assigned to the group profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Group Profile for Defining L2TP Attributes on page 487
- Configuring L2TP for a Group Profile on page 488
- Configuring the PPP Attributes for a Group Profile on page 488

hardware-address

Syntax hardware-address *mac-address*;

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6) **host** *hostname*]

Release Information Statement introduced in Junos OS 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***—MAC address of the client.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

host (Address-Assignment Pools)

Syntax

```
host hostname {
  hardware-address mac-address;
  ip-address ip-address;
}
```

Hierarchy Level [edit access address-assignment **pool** *pool-name* family (inet | inet6)]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure a static binding for the specified client.

Options ***hostname***—Name of the client.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools

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 OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the idle timeout for a user. The router might consider a PPP session to be idle because of the following reasons:

- There is no ingress traffic on the PPP session.
- There is no egress traffic.
- There is neither ingress or egress traffic on the PPP session
- There is no ingress or egress PPP control traffic. This is applicable only if keepalives are enabled.

Options *seconds*—Number of seconds a user can remain idle before the session is terminated.

Range: 0 through 4,294,967,295 seconds

Default: 0

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

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 OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router or switch processes the attributes it receives from the external server.

Options **framed-ip-netmask**—Ignore Framed-IP-Netmask (RADIUS attribute 9).

input-filter—Ignore Ingress-Policy-Name (VSA 26-10).

logical-system-routing-instance—Ignore Virtual-Router (VSA 26-1).

output-filter—Ignore Egress-Policy-Name (VSA 26-11).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access

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 OS Release 7.4.
ike-policy statement introduced in Junos OS Release 8.2.

Description Configure an IKE access profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IKE Access Profile on page 513

ike-policy

Syntax ike-policy *policy-name*;

Hierarchy Level [edit access profile *profile-name* client *client-name* ike]

Release Information Statement introduced in Junos OS 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 OS Services Interfaces Configuration Guide*.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IKE Access Profile on page 513
- *Junos IPsec Feature Guide*
- *Junos OS Services Interfaces Configuration Guide*

immediate-update

Syntax immediate-update;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the router or switch 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access
- Configuring Per-Subscriber Session Accounting

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 OS Release 8.3.

Description Detect inactive peers on dynamic IPsec tunnels.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IKE Access Profile on page 513

interface-description-format

Syntax

```
interface-description-format {
   exclude-adapter;
   exclude-sub-interface;
}
```

Hierarchy Level [edit access profile *profile-name* radius **options**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Options **exclude-adapter** and **exclude-sub-interface** introduced in Junos OS Release 10.4.

Description Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the device includes both the subinterface and the adapter in the interface description.

Options **exclude-adapter**—Exclude the adapter from the interface description.

exclude-sub-interface—Exclude the subinterface from the interface description.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- RADIUS Server Options for Subscriber Access

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 OS 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 OS Services Interfaces Configuration Guide*.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP for a Group Profile on page 488
- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring L2TP Properties for a Client-Specific Profile on page 495
- Configuring PPP Properties for a Client-Specific Profile on page 499
- Configuring an IKE Access Profile on page 513

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 OS Release 9.0.

Description Specify the reserved IP address assigned to the client.

Options ***ip-address***—IP version 4 (IPv4) address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools
- Configuring Static Address Assignment

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 OS Release 7.4.

Description Configure the keepalive interval for an L2TP tunnel.

Options ***seconds***—The time period that must elapse before the Junos OS 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

keepalive-retries

Syntax keepalive-retries *number-of-retries*;

Hierarchy Level [edit access profile *profile-name* client *client-name* ppp]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure the number of retry attempts for checking the keepalive status of a Point-to-Point (PPP) protocol session. Configure this setting to reduce the detection time for PPP client session timeouts or failures if you have configured the keepalive timeout interval (using the **keepalive** statement).

Options ***number-of-retries***—The maximum number of retries the L2TP network server (LNS) attempts by sending LCP echo requests to the peer to check the keepalive status of the PPP session. If there is no response from the PPP client within the specified number of retries, the PPP session is considered to have timed out.

Range: 3 through 32,767 times

Default: 10 times

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring PPP Properties for a Client-Specific Profile on page 499
- **keepalive on page 547**

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 OS Release 7.4.

Description Configure the Layer 2 Tunneling Protocol for a group profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP for a Group Profile on page 488

l2tp (Profile)

Syntax

```
l2tp {
  interface-id interface-id;
  lcp-renegotiation;
  local-chap;
  maximum-sessions-per-tunnel number;
  multilink {
    drop-timeout milliseconds;
    fragment-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 OS Release 7.4.

Description Configure the L2TP properties for a profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP Properties for a Client-Specific Profile on page 495

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 OS Release 7.4.

Description Configure the L2TP network server (LNS) so it renegotiates the link control protocol (LCP) with the PPP client.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP for a Group Profile on page 488
- Configuring L2TP Properties for a Client-Specific Profile on page 495

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 OS Release 7.4.

Description Configure the Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP for a Group Profile on page 488
- Configuring L2TP Properties for a Client-Specific Profile on page 495

maximum-lease-time

Syntax maximum-lease-time *seconds*;

Hierarchy Level [edit access address-assignment pool *pool-name* family (inet | inet6) **dhcp-attributes**]

Release Information Statement introduced in Junos OS 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***—Maximum number of seconds the lease can be held.

Range: 30 through 4,294,967,295 seconds

Default: 86,400 (24 hours)

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

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 OS Release 7.4.

Description Configure the maximum sessions for a Layer 2 tunnel.

Options ***number***—Maximum number of sessions for a Layer 2 tunnel.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP for a Group Profile on page 488
- Configuring L2TP Properties for a Client-Specific Profile on page 495

multilink

Syntax

multilink {
  drop-timeout *milliseconds*;
  fragment-threshold *bytes*;
}

Hierarchy Level [edit access **profile** *profile-name* **client** *client-name* **l2tp**]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure Multilink PPP for Layer 2 Tunneling Protocol (L2TP).

Options The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP Properties for a Client-Specific Profile on page 495

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

nas-identifier

Syntax nas-identifier *identifier-value*;

Hierarchy Level [edit access profile *profile-name* radius **options**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.

Options ***identifier-value***—String to use for authentication and accounting requests.

Range: 1 through 64 characters

Required Privilege Level admin—To view this statement in the configuration.
admin–control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access

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 OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

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.

NOTE: The total of the widths must not exceed 32 bits, or the configuration will fail.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access

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 OS Release 9.0.

Description Specify the NetBIOS node type. This is equivalent to DHCP option 46.

Options ***node-type***—One of the following node types:

- **b-node**—Broadcast node
- **h-node**—Hybrid node
- **m-node**—Mixed node
- **p-node**—Peer-to-peer node

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

network

Syntax network *ip-prefix*<*/prefix-length*>;

Hierarchy Level [edit access address-assignment **pool** *pool-name* family inet]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure subnet information for an IPv4 address-assignment pool.

Options

- ***ip-prefix***—IP version 4 address or prefix value.
- ***prefix-length***—(Optional) Subnet mask.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

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 | inet6) **dhcp-attributes**]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify user-defined options that are added to client packets.

Options

array—An option can include an array of option types.

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: byte, flag, integer, ip-address, short, string, unsigned-integer, or unsigned-short.

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).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

option-82 (Address-Assignment Pools)

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

options

Syntax

```
options {
  accounting-session-id-format (decimal | description);
  client-accounting-algorithm (direct | round-robin);
  client-authentication-algorithm (direct | round-robin);
  ethernet-port-type-virtual;
  interface-description-format {
    exclude-adapter;
    exclude-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;
  }
  revert-interval interval;
  vlan-nas-port-stacked-format;
}
```

Hierarchy Level [edit access profile *profile-name* **radius**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the options used by RADIUS authentication and accounting servers.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access
- RADIUS Server Options for Subscriber Access

order

Syntax order [*accounting-method*];

Hierarchy Level [edit access profile *profile-name* **accounting**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Set the order in which the Junos OS tries different accounting methods for client activity. When a client logs in, the software tries the accounting 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. The only valid value is **radius** for RADIUS accounting.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access

pap-password

Syntax pap-password *password*;

Hierarchy Level [edit access profile *profile-name* **client** *client-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the Password Authentication Protocol (PAP) password.

Options ***password***—PAP password.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PAP Password for an L2TP Profile on page 498

pool (Address-Assignment Pools)

Syntax

```
pool pool-name {
  family family {
    dhcp-attributes {
      [ protocol-specific attributes ]
    }
    host hostname {
      hardware-address mac-address;
      ip-address ip-address;
    }
    network ip-prefix/<prefix-length>;
    prefix ipv6-prefix;
    range range-name {
      high upper-limit;
      low lower-limit;
      prefix-length prefix-length;
    }
  }
  link pool-name;
}
```

Hierarchy Level [edit access **address-assignment**]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure the name of an address-assignment pool.

Options ***pool-name***—Name assigned to the address-assignment pool.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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)

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access

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 OS Release 7.4.

Description Configure PPP properties for a group profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488

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 OS Release 7.4.

Description Configure PPP properties for a client profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring PPP Properties for a Client-Specific Profile on page 499

ppp-authentication

Syntax ppp-authentication (chap | pap);

Hierarchy Level [edit access profile *profile-name* client *client-name* **l2tp**]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP authentication.

Options

- **chap**—Challenge Handshake Authentication Protocol.
- **pap**—Password Authentication Protocol.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP Properties for a Client-Specific Profile on page 495

ppp-profile

Syntax ppp-profile *profile-name*;

Hierarchy Level [edit access profile *profile-name* client *client-name* l2tp]

Release Information Statement introduced in Junos OS Release 7.4.

Description Specify the profile used to validate PPP session requests through L2TP tunnels.

Options ***profile-name***—Identifier for the PPP profile.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication for an L2TP Client and Profile on page 512

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IKE Access Profile on page 513

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 OS Release 7.4.

Description Configure the primary Domain Name System (DNS) server.

Options ***primary-dns***—An IPv4 address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

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 OS Release 7.4.

Description Configure the primary Windows Internet name server.

Options ***primary-wins***—An IPv4 address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

profile

Syntax

```
profile profile-name {
  accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    coa-immediate-update;
    immediate-update;
    order [ accounting-method ];
    statistics (time | volume-time);
    update-interval minutes;
    }
  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 string-value;
    }
    l2tp {
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      multilink {
        drop-timeout milliseconds;
        fragment-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 {
```



```
accounting-server [ ip-address ];
authentication-server [ ip-address ];
options {
  accounting-session-id-format (decimal | description);
  client-accounting-algorithm (direct | round-robin);
  client-authentication-algorithm (direct | round-robin);
  ethernet-port-type-virtual;
  interface-description-format {
    exclude-adapter;
    exclude-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;
  }
  revert-interval interval;
  vlan-nas-port-stacked-format;
}
attributes {
  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 ];
    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-filter [ accounting-start | accounting-stop ];
    output-gigapackets [ accounting-stop ];
    output-gigawords [ accounting-stop ];
  }
  ignore {
    framed-ip-netmask;
    input-filter;
    logical-system:routing-instance;
    output-filter;
```

```
            }
        }
    }
    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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Authentication Protocol on page 480
- Configuring Access Profiles for L2TP or PPP Parameters on page 490
- Configuring L2TP Properties for a Client-Specific Profile on page 495
- Configuring PPP Properties for a Client-Specific Profile on page 499

- AAA Service Framework Overview

radius (Access Profile)

Syntax

```
radius {
  accounting-server [ ip-address ];
  attributes {
    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 ];
      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-filter [ accounting-start | accounting-stop ];
      output-gigapackets [ accounting-stop ];
      output-gigawords [ accounting-stop ];
    }
    ignore {
      framed-ip-netmask;
      input-filter;
      logical-system-routing-instance;
      output-filter;
    }
  }
  authentication-server [ ip-address ];
  options {
    accounting-session-id-format (decimal | description);
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    ethernet-port-type-virtual;
    interface-description-format {
      exclude-adapter;
      exclude-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;
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
    }
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access
- RADIUS Server Options for Subscriber Access

radius-disconnect

Syntax

```
radius-disconnect {
    client-address {
        secret password;
    }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the RADIUS Disconnect Server for L2TP on page 511

radius-disconnect-port

Syntax radius-disconnect-port *port-number*;

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS 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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the RADIUS Disconnect Server for L2TP on page 511

radius-server

Syntax

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],
[edit access **profile** *profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication for L2TP on page 505
- Configuring the PPP Authentication Protocol on page 480
- Configuring RADIUS Authentication on page 103
- Configuring Authentication and Accounting Parameters for Subscriber Access

range (Address-Assignment Pools)

Syntax

range *range-name* {
  high *upper-limit*;
  low *lower-limit*;
  prefix-length *prefix-length*;
}

Hierarchy Level

[edit access address-assignment pool *pool-name* family (inet | inet6)]

Release Information

Statement introduced in Junos OS Release 9.0.
IPv6 support introduced in Junos OS Release 10.0.

Description

Configure a named range of IPv4 addresses or IPv6 prefixes, used within an address-assignment pool.

Options

high *upper-limit*—Upper limit of an address range or IPv6 prefix range.

low *lower-limit*—Lower limit of an address range or IPv6 prefix range.

prefix-length *prefix-length*—Assigned length of the IPv6 prefix.

range-name—Name assigned to the range of IPv4 addresses or IPv6 prefixes.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Address-Assignment Pools Overview
- Configuring Address-Assignment Pools

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 OS Release 9.0.

Description Specify the address-assignment pool named range to use based on the particular option 82 Agent Remote ID value.

Options **range *named-range***—Name of the address-assignment pool range to use.

value—String for Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) in DHCP packets.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the number of times that the router or switch 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Router or Switch Interaction with RADIUS Servers
- Example: Configuring CHAP Authentication with RADIUS on page 481
- Configuring RADIUS Authentication for L2TP on page 505
- **timeout on page 579**

revert-interval

Syntax revert-interval *interval*;

Hierarchy Level [edit access profile *profile-name* radius **options**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the amount of time the router or switch waits after a server has become unreachable. The router or switch rechecks the connection to the server when the specified 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: 0 through 4294967295 seconds

Default: 60 seconds

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring Authentication and Accounting Parameters for Subscriber Access

router (Address-Assignment Pools)

Syntax router [*router-address*];

Hierarchy Level [edit access address-assignment pool *pool-name* family inet **dhcp-attributes**]

Release Information Statement introduced in Junos OS Release 9.0.

Description Specify one or more routers located on the client's subnet. This statement is the equivalent of DHCP option 3.

Options ***router-address***—IP address of one or more routers.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the routing instance used to send RADIUS packets to the RADIUS server.

Options *routing-instance-name*—Routing instance name.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Authentication Protocol on page 480
- Configuring Authentication and Accounting Parameters for Subscriber Access

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 OS Release 7.4.

Description Configure the secondary DNS server.

Options *secondary-dns*—An IPv4 address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

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 OS Release 7.4.

Description Configure the secondary Windows Internet name server.

Options ***secondary-wins***—An IPv4 address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the PPP Attributes for a Group Profile on page 488
- Configuring PPP Properties for a Client-Specific Profile on page 499

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.

Options ***password***—Password to use; it can include spaces if the character string is enclosed in quotation marks.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Router or Switch Interaction with RADIUS Servers
- Example: Configuring CHAP Authentication with RADIUS on page 481
- Configuring RADIUS Authentication for L2TP on page 505
- Configuring the RADIUS Disconnect Server for L2TP on page 511

shared-secret

Syntax shared-secret *shared-secret*;

Hierarchy Level [edit access profile *profile-name* client *client-name* l2tp]

Release Information Statement introduced in Junos OS Release 7.4.

Description Configure the shared secret.

Options ***shared-secret***—The shared secret key for authenticating the peer.

Required Privilege Level admin—To view this statement in the configuration.
admin–control—To add this statement to the configuration.

Related Documentation

- Configuring L2TP Properties for a Client-Specific Profile on page 495

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

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***—Valid IPv4 address configured on one of the router or switch interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access
- Example: Configuring CHAP Authentication with RADIUS on page 481
- Configuring RADIUS Authentication for L2TP on page 505

statistics

Syntax statistics (time | volume-time);

Hierarchy Level [edit access profile *profile-name* **accounting**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Option **volume-time** introduced in Junos OS Release 9.4.

Description Configure the router or switch to collect time statistics, or both volume and time statistics, for the sessions being managed by AAA.

Options **time**—Collect uptime statistics only.

volume-time—Collect both volume and uptime statistics. This option is not available for Mobile IP.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Mobile IP Home Agent Elements and Behavior
- Configuring Authentication and Accounting Parameters for Subscriber Access

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

timeout (RADIUS)

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the amount of time that the local router or switch waits to receive a response from a RADIUS server.

Options ***seconds***—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access
- Example: Configuring CHAP Authentication with RADIUS on page 481
- Configuring RADIUS Authentication for L2TP on page 505

update-interval

Syntax update-interval *minutes*;

Hierarchy Level [edit access profile *profile-name* **accounting**]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the amount of time that the router or switch waits before sending a new accounting update.

Default No updates

Options *minutes*—Amount of time between updates, in minutes.

Range: 10 through 1440 minutes

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Applying a Configured PPP Group Profile to a Tunnel on page 501

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 OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring Authentication and Accounting Parameters for Subscriber Access

wins-server

Syntax

```
wins-server {
  ipv4-address;
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family inet **dhcp-attributes**]

Release Information Statement introduced in Junos OS 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 ***ipv4-address***—IP address of each NetBIOS name server; add them to the configuration in order of preference.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Address-Assignment Pools

PART 4

Security Services

CHAPTER 16

Security Services Overview

This chapter includes the following topics:

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 OS 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 Feature Guide*.

Related Documentation

- IPsec Configuration for an ES PIC Overview on page 593
- Security Associations Overview on page 585

Security Associations Overview

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 OS implementation of IPsec supports two modes of security (transport and tunnel).

Related Documentation

- IKE Key Management Protocol Overview on page 586
- IPsec Requirements for Junos-FIPS on page 586
- Security Services Configuration Statements on page 589

IKE Key Management Protocol Overview

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.

Related Documentation

- Security Associations Overview on page 585
- IPsec Requirements for Junos-FIPS on page 586
- Security Services Configuration Statements on page 589

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.

Related Documentation

- Security Associations Overview on page 585
- IKE Key Management Protocol Overview on page 586
- Security Services Configuration Statements on page 589

CHAPTER 17

Security Services Configuration Guidelines

This chapter includes the following topics:

Security Services Configuration Statements

To configure security services, you can include the following configuration 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 {
    auto-re-enrollment {
      certificate-id {
        ca-profile ca-profile-name;
        challenge-password password;
        re-enroll-trigger-time-percentage percentage;
        re-generate-keypair;
        validity-period days;
      }
    }
    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;
          }
        }
      }
```

```
  }
  traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
  }
}
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 OS System Basics and Services Command Reference*.

Related Documentation

- Security Services Configuration Statements

Configuring IPsec for an ES PIC

- Configuring the IPsec Policy for an ES PIC on page 609
- Example: Configuring an IPsec Policy on page 610

IPsec Configuration for an ES PIC Overview

IPsec provides a secure way to authenticate senders and encrypt IPv4 and IPv6 traffic between network devices, such as routers 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.

Related Documentation

- Configuring Minimum Manual Security Associations for IPsec on an ES PIC on page 593
- Configuring Minimum Digital Certificate Requirements for IKE on an ES PIC on page 594
- Enabling Dynamic IPsec Security Associations on page 594
- Configuring an IKE Proposal for Dynamic SAs on page 601
- Example: Configuring an IKE Proposal on page 604

Configuring Minimum Manual Security Associations for IPsec on an ES PIC

To define a manual security association (SA) configuration for an ES PIC, 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;
    }
  }
}
```

Related Documentation

- IPsec Configuration for an ES PIC Overview on page 593

Configuring Minimum IKE Requirements for IPsec on an ES PIC

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);
}
```

Related Documentation

- IPsec Configuration for an ES PIC Overview on page 593

Configuring Minimum Digital Certificate Requirements for IKE on an ES PIC

To define a digital certificate configuration for IKE for an encryption interface on M Series and T Series routers, 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;
  }
}
```

Related Documentation

- IPsec Configuration for an ES PIC Overview on page 593

Configuring Security Associations for IPsec on an ES PIC

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 IPsec Security Associations for an ES PIC” on page 597.
- Dynamic—Specify 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 “Associating the Configured Security Association with a Logical Interface” on page 621.

NOTE: The Junos OS 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;
```

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 OS Feature Guides* and the “IPsec Services Configuration Guidelines” chapter of the *Junos OS Services Interfaces Configuration Guide*.

Tasks to configure SAs for IPsec for an ES PIC are:

1. Configuring the Description for an SA on page 595
2. Configuring IPsec Transport Mode on page 595
3. Configuring IPsec Tunnel Mode on page 596
4. Configuring Manual IPsec Security Associations for an ES PIC on page 597
5. Configuring Dynamic IPsec Security Associations on page 601
6. Enabling Dynamic IPsec Security Associations on page 601

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 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 OS 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.

NOTE: You can configure BGP to establish a peer relationship over encrypted tunnels.

Configuring IPsec Tunnel Mode

You use tunnel mode when you use preshared keys with IKE to authenticate peers, or digital certificates with IKE to authenticate peers.

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: The Junos OS supports both both BGP and OSPFv3 in transport mode.

To enable tunnel mode, follow the steps in these sections:

- Enabling Dynamic IPsec Security Associations on page 594
- Configuring an IKE Proposal for Dynamic SAs on page 601
- Associating the Configured Security Association with a Logical Interface on page 621
- IPsec Tunnel Traffic Configuration Overview on page 631

Configuring Manual IPsec Security Associations for an ES PIC

To use IPsec security services, you create security associations (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. 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;
  }
}
```

Tasks to configure a manual SA are:

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);
```


The following example shows how to define different algorithms, keys, and security parameter index values for inbound and outbound processing directions:

```
[edit security ipsec security-association sa-name]
manual {
  direction inbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 2345678901234567890l234;
    }
    protocol esp;
    spi 16384;
  }
  direction outbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 12345678901234567890abcd;
    }
    protocol esp;
    spi 24576;
  }
}
```

The following example shows how to define the same algorithms, keys, and security parameter index values for bidirectional processing:

```
[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 routers.

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.

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 OS 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 IPsec 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 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);
}
```

Enabling Dynamic IPsec Security Associations

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.

NOTE: Dynamic tunnel SAs require an ES PIC. 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 for Dynamic SAs

Dynamic Security Associations (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 “Configuring an IKE Policy for Preshared Keys” on page 604.

Tasks for configuring the IKE proposal are:

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**—Specify that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specify 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

The following example shows how to 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;
}
```

Related Documentation

- Configuring an IKE Proposal for Dynamic SAs on page 601

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.

Tasks for configuring an IKE policy are:

1. Configuring the Description for an IKE Policy on page 605
2. Configuring the Mode for an IKE Policy on page 605
3. Configuring the Preshared Key for an IKE Policy on page 605
4. Associating Proposals with an IKE Policy on page 605

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. A commit operation fails if either a preshared key or a 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 ];
```

Related Documentation

- Example: Configuring an IKE Policy on page 606

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 OS System Basics and Services Command Reference*.

Related Documentation

- Configuring an IKE Policy for Preshared Keys on page 604

Configuring an IPsec Proposal for an 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);
}
```

Tasks to configure an IPsec proposal for an ES PIC are:

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 for an 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 ];
}
```

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**—Specify that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specify 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.

Related Documentation

- Example: Configuring an IPsec Policy on page 610
- IPsec Configuration for an ES PIC Overview on page 593

Example: Configuring an IPsec Policy

The following example shows how to configure an IPsec policy:

```
[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 OS System Basics and Services Command Reference*.

Related Documentation

- Configuring the IPsec Policy for an ES PIC on page 609
- IPsec Configuration for an ES PIC Overview on page 593

Using Digital Certificates for ES and AS PICs

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 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 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.

Related Documentation

- Configuration Statements for Configuring Digital Certificates for an ES PIC on page 612
- Obtaining a Certificate from a Certificate Authority for an ES PIC on page 613
- Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 613
- Generating a Private and Public Key Pair for Digital Certificates for an ES PIC on page 614
- Configuring Digital Certificates for an ES PIC on page 614
- Configuring an IKE Policy for Digital Certificates for an ES PIC on page 619
- Associating the Configured Security Association with a Logical Interface on page 621

Configuration Statements for Configuring Digital Certificates for an ES PIC

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 ];
    }
}
```

The statements for configuring digital certificates differ for the AS and MultiServices PICs and the ES PIC.

For information about how to configure the **description** and **mode** statements, see "Configuring the Description for an IKE Policy" on page 605 and "Configuring the Mode for an IKE Policy" on page 605. For information about how to configure the IKE proposal, see "Associating Proposals with an IKE Policy" on page 605

NOTE: **For digital certificates, the Junos OS supports only VeriSign CAs for the ES PIC.**

Related Documentation

- Digital Certificates Overview on page 611

Obtaining a Certificate from a Certificate Authority for an 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 OS supports only the Simple Certificate Enrollment Protocol (SCEP).**

Related Documentation

- Digital Certificates Overview on page 611

Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router

For an encryption interface on an M Series or T Series router, 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
```

Related Documentation

- Example: Requesting a CA Digital Certificate on page 614

- Digital Certificates Overview on page 611

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://*hostname/path/filename*
URL: http://*hostname/path/filename* 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.

Related Documentation

- Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 613

Generating a Private and Public Key Pair for Digital Certificates for an ES PIC

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 OS only supports RSA.

The following example shows how to generate a private and public key pair:

user@host> **request security key-pair batt**
Generated key pair, key size 1024, file batt Algorithm RSA

Related Documentation

- Digital Certificates Overview on page 611

Configuring Digital Certificates for an ES PIC

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.

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 ];
  }
}
```

Tasks to configure digital certificates for ES PICs are:

Configuring the Certificate Authority Properties for an ES PIC

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.

Tasks for configuring the CA properties are:

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 or switch sends 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 or switch 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 or switch 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 for an 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;
}
```

Tasks for configuring an IKE policy for digital certificates are:

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 for an ES PIC

To obtain a 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.

The following example shows how to 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 OS 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
```

Related Documentation

- Digital Certificates Overview on page 611

Associating the Configured Security Association with a Logical Interface

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.

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.

The following example shows how to 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
    }
  }
}
```

Related Documentation

- Enabling Dynamic IPsec Security Associations on page 594

Configuring Digital Certificates for Adaptive Services Interfaces

A digital certificate implementation uses the public key infrastructure (PKI), which requires that you 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 that a certificate authority (CA) send you a CA certificate that contains the public key of the CA. Next you request that the CA enroll you 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 router and load the CA in remote devices before you can establish IPsec tunnels with your peers.

NOTE: For digital certificates, the Junos OS 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 routers, 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;
        }
      }
    }
  }
}
```

The following tasks enable you to implement digital certificates on J Series Services Routers and AS and MultiServices PICs installed on M Series and T Series routers:

1. Configuring the Certificate Authority Properties on page 623
2. Configuring the Certificate Revocation List on page 625
3. Managing Digital Certificates on page 626
4. Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 628

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;
    }
}
```

Tasks for configuring the Certificate Authority properties are:

1. Specifying the CA Profile Name on page 624
2. Specifying an Enrollment URL on page 624
3. Specifying the Enrollment Properties on page 624

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 routers.

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

Tasks to configure the certificate revocation list are:

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 router 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.

Tasks to manage digital certificates are:

1. Requesting a CA Digital Certificate for AS and MultiServices PICs installed on M Series and T Series Routers on page 626
2. Generating a Public/Private Key Pair on page 627
3. Generating and Enrolling a Local Digital Certificate on page 627

Requesting a CA Digital Certificate for AS and MultiServices PICs installed on M Series and T Series Routers

For J Series Services Routers and AS and MultiServices PICs installed on M Series and T Series routers, 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 623.

In this example, the certificate is enrolled online and installed into the router 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 OS 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.

The following example shows how to 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 router, issue the **request security pki local-certificate load** command.

The following example shows how to 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+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjAOBgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5SOQXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH406gQ3G
3iHOZfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteolZCiZ70f09Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----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 router 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 router.

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.

Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA

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 automatic reenrollment 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 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.

Tasks to configure automatic reenrollment of certificates are:

1. Specify the Certificate ID on page 629
2. Specify the CA Profile on page 629
3. Specify the Challenge Password on page 630
4. Specify the Reenroll Trigger Time on page 630
5. Specify the Regenerate Key Pair on page 630
6. Specify the Validity Period on page 630

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.

Related Documentation

- Digital Certificates Overview on page 611
- Configuring Digital Certificates for an ES PIC on page 614

Configuring IPsec Tunnel Traffic

This section includes the following topics:

- Example: Configuring an Inbound Traffic Filter for a Policy Check on page 634
- Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check on page 634

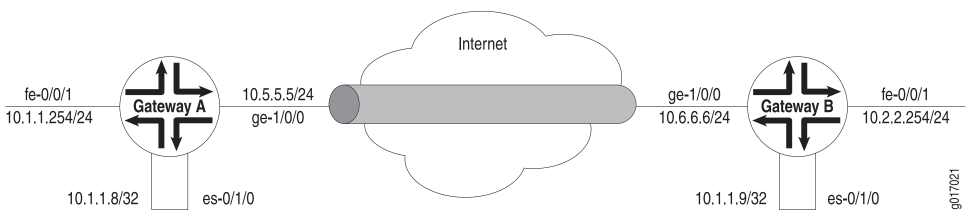
IPsec Tunnel Traffic Configuration Overview

Traffic configuration defines the traffic that must flow through the IPsec 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 10 on page 631, 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.

Figure 10: Example: IPsec Tunnel Connecting Security Gateways



The SA and ES interfaces for 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 interfaces for 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 123456789009876543211234;
                }
            }
        }
    }
    [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;
            }
        }
    }
```

Related Documentation

- Example: Configuring an Outbound Traffic Filter on page 632
- Example: Applying an Outbound Traffic Filter on page 633
- Example: Configuring an Inbound Traffic Filter for a Policy Check on page 634
- ES Tunnel Interface Configuration for a Layer 3 VPN on page 635

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 10 on page 631). 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.

Related Documentation

- Example: Applying an Outbound Traffic Filter on page 633
- IPsec Tunnel Traffic Configuration Overview on page 631

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.

Related Documentation

- IPsec Tunnel Traffic Configuration Overview on page 631

Example: Configuring an Inbound Traffic Filter for a 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;
```

Related Documentation

- IPsec Tunnel Traffic Configuration Overview on page 631

Example: Applying an Inbound Traffic Filter to an ES PIC for a 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.

Related Documentation

- IPsec Tunnel Traffic Configuration Overview on page 631

ES Tunnel Interface Configuration 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.

Related Documentation

- IPsec Tunnel Traffic Configuration Overview on page 631

Configuring Tracing Operations for Security Services

To configure trace options for security services, 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 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

Related Documentation

- Configuring Tracing Operations for IPsec Events for Adaptive Services PICs on page 636
- Security Associations Overview on page 585

Configuring Tracing Operations for IPsec Events for Adaptive Services PICs

To configure trace options to trace IPsec events for Adaptive Services PICs, include the following statements at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
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;
}
```

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

Related Documentation

- Configuring Tracing Operations for Security Services on page 635

Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols

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.

The following topics provide more details about configuring authentication key updates for BGP and LDP Routing Protocols:

1. Configuring Authentication Key Updates on page 637
2. Configuring BGP and LDP for Authentication Key Updates on page 638

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 keychain 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 keychain 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 keychain 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 keychain.

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: 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 OS Routing Protocols Configuration Guide*.

Related Documentation

- Example: Configuring the BGP and IS-IS Routing Protocols on page 274

Configuring SSH Host Keys for Secure Copying of Data

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.

Tasks to configure SSH host keys for secure copying of data are:

1. Configuring SSH Known Hosts on page 639
2. Configuring Support for SCP File Transfer on page 639
3. Updating SSH Host Key Information on page 640

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 OS 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 OS 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@switch# 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.

1. Retrieving Host Key Information Manually on page 640
2. Importing Host Key Information from a File on page 640

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@switch# 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@switch# set security ssh-known-hosts load-key-file /var/tmp/known-hosts
```

Importing SSL Certificates for Junos XML Protocol Support

A Junos XML protocol client application can use one of four protocols to connect to the Junos XML protocol server on a router or switch: clear-text (a Junos XML protocol-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 or switch, as described in this topic. You must also include the **xnm-ssl** statement at the **[edit system services]** hierarchy level.

NOTE: **The xnm-ssl statement does not apply to standard IPsec services.**

After obtaining an X.509 authentication certificate and private key, copy it to the router or switch 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, **Junos XML protocol-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 or switch'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 Junos XML protocol client application runs).

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.

Related Documentation

- Configuring SSH Host Keys for Secure Copying of Data on page 638
- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 189

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;
               }
            }
         }
      }
```



```
    }
}
```

Tasks for configuring internal IPsec for Junos-FIPS are:

1. Configuring the SA Direction on page 642
2. Configuring the IPsec SPI on page 643
3. Configuring the IPsec Key on page 643

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 "$.KL3rngIH7,theOPcn87lxfpe9GJKdme";
                    }
                }
                direction outbound {
                    protocol esp;
                    spi 513;
                    encryption {
                        algorithm 3des-cbc;
                        key ascii-text ".n87lngIH7,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.

Related Documentation

- Example: Configuring Internal IPsec on page 643

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";
          }
        }
      }
    }
  }
}
```

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641

CHAPTER 18

Summary of Security Services Configuration Statements

The following configuration statement references explain each of the security services configuration statements. The statement references are organized alphabetically.

algorithm (Authentication Keychain)

Syntax algorithm (hmac-sha-1 | md5);

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure the authentication algorithm for IS-IS.

Options **hmac-sha-1**—96-bit hash-based message authentication code (SHA-1).

md5—Message digest 5.

Default: md5

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Hitless Authentication Key Rollover for IS-IS
- Overview of Hitless Authentication Key Rollover for IS-IS

algorithm (Junos FIPS)

Syntax algorithm 3des-cbc;

Hierarchy Level [edit security ipsec internal security-association manual direction encryption]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level Crypto Officer—To add and view this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 597

authentication-algorithm (IKE)

Syntax authentication-algorithm (md5 | sha1);

Hierarchy Level [edit security ike **proposal** *ike-proposal-name*]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the Authentication Algorithm for an IKE Proposal on page 602

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the Authentication Algorithm for an IPsec Proposal on page 607

authentication-key-chains

Syntax

```
authentication-key-chains {
  key-chain key-chain-name {
    description text-string;
    key key {
      algorithm (md5 | hmac-sha-1);
      options (basic | isis-enhanced);
      secret secret-data;
      start-time yyyy-mm-dd.hh:mm:ss;
    }
    tolerance seconds;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the **authentication-key-chains** statement is configured at the **[edit security]** hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the **[edit protocols]** hierarchy level or with the BFD protocol using the **bfd-liveness-detection** statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication Key Updates on page 637
- Configuring BFD Authentication for Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS

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 OS 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 597

auto-re-enrollment

Syntax

```
auto-re-enrollment {
  certificate-id {
    ca-profile ca-profile-name;
    challenge-password password;
    re-enroll-trigger-time-percentage percentage;
    re-generate-keypair;
    validity-period days;
  }
}
```

Hierarchy Level [edit security pki]

Release Information Statement introduced in Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 628
- Configuring Digital Certificates for Adaptive Services Interfaces on page 622

auxiliary-spi

Syntax auxiliary-spi *auxiliary-spi-value*;

Hierarchy Level [edit security ipsec security-association *sa-name* manual **direction** (inbound | outbound | bi-directional)]

Release Information Statement introduced before Junos OS 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 597
- **spi on page 701**

ca-identity

Syntax ca-identity *ca-identity*;

Hierarchy Level [edit security **pki ca-profile** *ca-profile-name*]

Release Information Statement introduced in Junos OS 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 routers.

Options ***ca-identity***—The name of the CA identity. This name is typically the domain name of the CA.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying the CA Profile Name on page 624

ca-name

Syntax ca-name *ca-identity*;

Hierarchy Level [edit security certificates **certification-authority**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the certificate authority (CA) identity to use in the certificate request.

Options ***ca-identity***—CA identity to use in the certificate request.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying the Certificate Authority Name on page 616

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 OS Release 7.5.
revocation-check and **crl** statements added in Junos OS 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 routers.

The remaining statements are explained separately.

Options ***ca-profile-name***—Name of the trusted CA.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying the CA Profile Name on page 624

cache-size

Syntax cache-size *bytes*;

Hierarchy Level [edit security **certificates**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches 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.**

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

Related Documentation

• Configuring the Cache Size on page 617

cache-timeout-negative

Syntax cache-timeout-negative *seconds*;

Hierarchy Level [edit security **certificates**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches 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.**

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

Related Documentation
- Configuring the Negative Cache on page 618

certificate-id

Syntax

```
certificate-id {
    ca-profile ca-profile-name;
    challenge-password password;
    re-enroll-trigger-time-percentage percentage;
    re-generate-keypair;
    validity-period days;
}
```

Hierarchy Level [edit security **auto-re-enrollment**]

Release Information Statement introduced in Junos OS 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.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 628
- **auto-re-enrollment on page 651**

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series and EX Series switches routers only) Configure the digital certificates for IPsec.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Digital Certificates for an ES PIC on page 614

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure a certificate authority profile name.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

Related Documentation
- Configuring the Certificate Authority Properties for an ES PIC on page 615

challenge-password

Syntax challenge-password *password*;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id]

Release Information Statement introduced in Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 628
- **auto-re-enrollment on page 651**

crl (Encryption Interface)

Syntax crl *file-name*;

Hierarchy Level [edit security **certificates**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) 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***—Specify the file from which to read the CRL.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

Related Documentation

- Configuring the Certificate Authority Properties for an ES PIC on page 615

crl (Adaptive Services Interface)

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 OS 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—Permit the authentication of the IPsec peer when the CRL is not downloaded.

password—Password to access the URLs.

refresh-interval ***number-of-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.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

Related Documentation

- Configuring the Certificate Revocation List on page 625

description (Authentication Keychain)

Syntax description *text-string*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description Configure a description for an authentication key-chain.

Options *text-string*—A text string describing the **authentication-key-chain**. Put the text string in quotes (“text description”).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication Key Updates on page 637
- Configuring BFD Authentication for Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS

description (IKE policy)

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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Enabling Dynamic IPsec Security Associations on page 594
- Configuring the Description for an IKE Proposal on page 602
- Configuring the Description for an IKE Policy on page 605
- Configuring an IPsec Proposal for an ES PIC on page 607
- Configuring the IPsec Policy for an ES PIC on page 609

dh-group

Syntax dh-group (group1 | group2);

Hierarchy Level [edit security ike **proposal** *ike-proposal-name*]

Release Information Statement introduced before Junos OS 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.
- **group5**—1536-bit.
- **group14**—2048-bit.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Diffie-Hellman Group for an IKE Proposal on page 603

direction (Junos OS)

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 OS Release 7.4.

Description Define the direction of IPsec processing.

Options

inbound—Inbound SA—Define algorithms, keys, or security parameter index (SPI) values to decrypt and authenticate incoming traffic coming from the peer.

outbound—Outbound SA—Define algorithms, keys, or SPI values to decrypt and authenticate outbound traffic to the peer.

bidirectional—Bidirectional SA—Decrypt and authenticate the incoming and outgoing traffic using the same algorithm, keys, or SPI in both directions, unlike inbound and outbound SAs that use different attributes in both directions.

The remaining 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 Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 597

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],
[edit security trusted-channel ipsec 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.

Required Privilege Level

Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Dynamic IPsec Security Associations on page 601
- Associating the Configured Security Association with a Logical Interface on page 621

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Type of Encoding Your CA Supports on page 616
- Configuring the Type of Encoding Your CA Supports on page 620

encryption (Junos OS)

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 OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 597

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 OS Release 7.4.

Description Define the encryption parameters for internal Routing-Engine–to–Routing-Engine communication. The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IKE Proposal for Dynamic SAs on page 601
- Configuring an IPsec Proposal for an ES PIC on page 607

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 OS 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 routers.

Options **url** ***url-name***—Location of the 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***—Length of time, in seconds, that a router should wait between enrollment attempts.

Range: 0 through 3600

Default: 0

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying an Enrollment URL on page 624
- Specifying the Enrollment Properties on page 624

enrollment-retry

Syntax enrollment-retry *attempts*;

Hierarchy Level [edit security **certificates**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.

Options ***attempts***—Number of enrollment retries.

Range: **0** through **100**

Default: **0**

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Number of Enrollment Retries on page 618

enrollment-url

Syntax enrollment-url *url-name*;

Hierarchy Level [edit security certificates **certification-authority** *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).

Options ***url-name***—Certificate authority URL.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying an Enrollment URL on page 617

file

Syntax file *certificate-filename*;

Hierarchy Level [edit security certificates **certification-authority** *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.

Options ***certificate-filename***—File from which to read the digital certificate.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying a File to Read the Digital Certificate on page 617

identity

Syntax identity *identity-name*;

Hierarchy Level [edit security ike]

Release Information Statement introduced before Junos OS 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).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Identity to Define the Remote Certificate Name on page 620

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 OS Release 7.4.

Description (Encryption interface on M Series and T Series routers only) Configure IKE.

Options The remaining 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 Documentation

- Configuring an IKE Proposal for Dynamic SAs on page 601
- Configuring an IKE Policy for Preshared Keys on page 604

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 OS Release 7.4.

Description (Junos-FIPS only) Define an internal security association (SA) for internal Routing-Engine–to–Routing-Engine communication.

Options The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *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 OS Release 7.4.

Description (Encryption interface on M Series and T Series routers only) Configure IPsec.

Options The remaining 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 Documentation

- Enabling Dynamic IPsec Security Associations on page 594

key (Authentication Keychain)

Syntax

```
key key {
  algorithm (md5 | hmac-sha-1);
  options (basic | isis-enhanced);
  secret secret-data;
  start-time yyyy-mm-dd.hh:mm:ss;
}
```

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name*]

Release Information
Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description Configure the authentication element.

Options *key*—Each key within a keychain is identified by a unique integer value.

Range: 0 through 63

The remaining statements are explained separately.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication Key Updates on page 637
- Configuring BFD Authentication for Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS

key (Junos FIPS)

Syntax key ascii-text *ascii-text-string*;

Hierarchy Level [edit security ipsec internal security-association manual direction encryption]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level Crypto Officer—To add and view this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

key-chain

Syntax

```
keychain key-chain-name {
  description text-string;
  key key {
    algorithm (md5 | hmac-sha-1);
    options (basic | isis-enhanced);
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
  }
  tolerance seconds;
}
```

Hierarchy Level [edit security authentication-key-chains]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description Create the key-chain configuration for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.

Options *key-chain-name*—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (“ ”).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- **authentication-key-chains on page 649**
- Configuring Authentication Key Updates on page 637
- Configuring BFD Authentication for Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS

ldap-url

Syntax <ldap-url *url-name*>;

Hierarchy Level [edit security certificates **certification-authority** *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.

Options ***url-name***—Name of the LDAP URL.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying an LDAP URL on page 617

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 OS 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Lifetime for an IKE SA on page 603
- Configuring the Lifetime for an IPsec SA on page 608

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.

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 *URL-or-path*—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 or switch's local disk)
- URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Importing SSL Certificates for Junos XML Protocol Support on page 640

local-certificate

Syntax local-certificate *certificate-filename*;

Hierarchy Level [edit security ike **policy** *ike-peer-address*]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Specifying the Certificate Filename on page 620

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***—Specify the file from which to read the private and public key pair.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Specifying the Private and Public Key File on page 620

manual (Junos OS)

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 OS Release 7.4.

Description Define a manual IPsec SA.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 597

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 OS 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.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches 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

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Maximum Number of Peer Certificates on page 618

mode (IKE)

Syntax mode (aggressive | main);

Hierarchy Level [edit security ike **policy** *ike-peer-address*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the IKE policy mode.

Default main

Options **aggressive**—Take half the number of messages of main mode, has less negotiation power, and does not provide identity protection.

main—Use 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Mode for an IKE Policy on page 605

mode (IPsec)

Syntax mode (transport | tunnel);

Hierarchy Level [edit security ipsec **security-association** *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the mode for the IPsec security association.

Default **tunnel**

Options **transport**—Protect 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—Protect traffic using preshared keys with IKE to authenticate peers or digital certificates with IKE to authenticate peers.

NOTE: The Junos OS supports only encapsulating security payload (ESP) when you use tunnel mode.

In transport mode, the Junos OS does not support authentication header (AH) and ESP header bundles.

In transport mode, the Junos OS supports only Border Gateway Protocol (BGP).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring IPsec Tunnel Mode on page 596

options

Syntax options (basic | isis-enhanced);

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 11.2.

Description For IS-IS only, configure the protocol transmission encoding format for encoding the message authentication code in routing protocol packets.

Because this setting is for IS-IS only, the TCP and the BFD protocol ignore the encoding option configured in the key.

Options **basic**—RFC 5304 based encoding. Junos OS sends and receives RFC 5304-encoded routing protocols packets, and drops 5310-encoded routing protocol packets that are received from other devices.

isis-enhanced—RFC 5310 based encoding. Junos OS sends RFC 5310-encoded routing protocol packets and accepts both RFC 5304-encoded and RFC 5310-encoded routing protocol packets that are received from other devices.

Default: basic

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Hitless Authentication Key Rollover for IS-IS
- Overview of Hitless Authentication Key Rollover for IS-IS

path-length

Syntax path-length *certificate-path-length*;

Hierarchy Level [edit security **certificates**]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificate path length.

Options ***certificate-path-length***—Digital certificate path length.

Range: 2 through 15 certificates

Default: 15 certificates

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the Path Length for the Certificate Hierarchy on page 618

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 OS Release 7.4.

Description Define the Perfect Forward Secrecy (PFS) protocol. Create 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Perfect Forward Secrecy on page 609

pki

Syntax

```
pki {
  auto-re-enrollment {
    certificate-id {
      ca-profile ca-profile-name;
      challenge-password password;
      re-enroll-trigger-time-percentage percentage;
      re-generate-keypair;
      validity-period days;
    }
  }
  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;
        }
      }
    }
  }
  traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 7.5.
revocation-check and **crl** statements added in Junos OS 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 routers.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Digital Certificates for Adaptive Services Interfaces on page 622

- *Junos OS Feature Guides*
- *Junos OS System Basics and Services Command Reference*

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IKE Policy for Preshared Keys on page 604
- Configuring an IKE Policy for Digital Certificates for an ES PIC on page 619

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 OS Release 7.4.

Description Define an IPsec policy.

Options ***ipsec-policy-name***—Specify an IPsec policy name.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the IPsec Policy for an ES PIC on page 609

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 OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring the Preshared Key for an IKE Policy on page 605

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 OS Release 7.4.

Description Define an IKE proposal for a dynamic SA.

Options *ike-proposal-name*—Specify an IKE proposal name.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IKE Proposal for Dynamic SAs on page 601

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 OS Release 7.4.

Description Define an IPsec proposal for a dynamic SA.

Options *ipsec-proposal-name*—Specify an IPsec proposal name.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring an IPsec Proposal for an ES PIC on page 607

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 OS Release 7.4.

Description Associate one or more proposals with an IKE or IPsec policy.

Options ***proposal-names***—Name of one or more proposals.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Associating Proposals with an IKE Policy on page 605
- Configuring the IPsec Policy for an ES PIC on page 609

protocol (Junos OS)

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 OS 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)

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Manual IPsec Security Associations for an ES PIC on page 597
- Configuring the Protocol for a Dynamic IPsec SA on page 608

protocol (Junos-FIPS Software)

Syntax protocol esp;

Hierarchy Level [edit security ipsec internal security-association manual direction]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level Crypto Officer—To add and view this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

re-enroll-trigger-time-percentage

Syntax re-enroll-trigger-time-percentage *percentage*;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id]

Release Information Statement introduced in Junos OS 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 628
- **auto-re-enrollment on page 651**

re-generate-keypair

Syntax <re-generate-keypair>;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id]

Release Information Statement introduced in Junos OS 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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 628
- **auto-re-enrollment on page 651**

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 OS 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Certificate Revocation List on page 625
- **crl on page 661**

retry

Syntax retry *number-of-attempts*;

Hierarchy Level [edit security pki ca-profile *ca-profile-name* enrollment]

Release Information Statement introduced in Junos OS 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying the Enrollment Properties on page 624
- **enrollment on page 670**

retry-interval

Syntax retry-interval *seconds*;

Hierarchy Level [edit security pki ca-profile *ca-profile-name* enrollment]

Release Information Statement introduced in Junos OS 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying the Enrollment Properties on page 624
- **enrollment on page 670**

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 OS 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 routers.

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.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Certificate Revocation List on page 625

secret

Syntax secret *secret-data*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description Specify a password in encrypted text or plain text format. The secret password always appears in encrypted format.

Options ***secret-data***—Password to use; it can include spaces if the character string is enclosed in quotation marks.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication Key Updates on page 637
- Configuring BFD Authentication for Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS

security-association (Junos OS)

Syntax

```
security-association sa-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);
  }
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an IPsec security association.

Options *sa-name*—Name of the security association.

The remaining 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 Documentation

- Enabling Dynamic IPsec Security Associations on page 594

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 OS Release 7.4.

Description Define a security association (SA) for internal Routing-Engine–to–Routing-Engine communication.

Options The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

spi (Junos OS)

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 OS Release 7.4.

Description Configure the security parameter index (SPI) for a security association (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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 597

spi (Junos-FIPS Software)

Syntax spi *spi-value*;

Hierarchy Level [edit security ipsec internal security-association manual direction]

Release Information Statement introduced before Junos OS 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

Required Privilege Level Crypto Officer—To add and view this statement in the configuration.

Related Documentation

- Configuring Internal IPsec for Junos-FIPS on page 641
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

ssh-known-hosts

Syntax

```
ssh-known-hosts {
  host host-name {
    dsa-key key;
    fetch-from-server host-name;
    load-key-file file-name;
    rsa-key key;
    rsa1-key key;
  }
}
```

Hierarchy Level [edit security ssh-known-hosts]

Release Information Statement introduced in Junos OS Release 7.5.

Description Configure SSH support for known hosts and for administering SSH host key updates.

Options **host *host-name***—Hostname of the SSH known host entry. This option has the following suboptions:

- **dsa-key *key***—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.
- **fetch-from-server *host-name***—Retrieve SSH public host key information from a specified server.
- **load-key-file *filename***—Import SSH host key information from the ***/var/tmp/ssh-known-hosts*** file.
- **rsa-key *key***—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.
- **rsa1-key *key***—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring SSH Host Keys for Secure Copying of Data on page 638

start-time

Syntax start-time *yyyy-mm-dd.hh:mm:ss*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description Specify a start time for key transmission. You do not need to specify an end time for the key. If a new key is present with a new start time, the keychain rolls over to the new one.

Options ***yyyy–mm-dd.hh:mm:ss***—Start time in UTC (Coordinated Universal Time). The start time must be unique within the keychain.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication Key Updates on page 637
- Configuring BFD Authentication for Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS

tolerance

Syntax tolerance *seconds*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description Configure the clock-skew tolerance for accepting keys for a key chain.

Options ***seconds***—Number of seconds to accept for clock-skew.

Default: 0 seconds

Range: 0 through 999,999,999

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication Key Updates on page 637
- Configuring BFD Authentication for Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS

traceoptions

Syntax

```
traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag certificates;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
  level
  no-remote-trace
}
```

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 OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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 *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all security events.
- **certificates**—Trace certificate 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.

level ***level***—(Optional) Set traceoptions level.

- **all**—match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing

Required Privilege Level

admin—To view the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Tracing Operations for Security Services on page 635

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 OS 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.

Required Privilege Level admin—To view the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying an Enrollment URL on page 624
- Specifying an LDAP URL on page 625
- **crl on page 661**
- **enrollment on page 670**

validity-period

Syntax validity-period *days*;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id]

Release Information Statement introduced in Junos OS Release 8.5.

Description 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

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 628
- **auto-re-enrollment on page 651**

PART 5

Router Chassis

CHAPTER 19

Router Chassis Configuration Guidelines

This chapter includes the following topics:

Router Chassis Configuration Statements

You can configure properties of the router chassis, including conditions that activate the red and yellow alarm LEDs 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 OS 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;
}
feb
    slot number
        ucode-imem-remap
    {
}
fpc slot-number {
    port-mirror-instance port-mirroring-instance-name;
    sampling-instance;
    power (off | on);
        pic pic-number {
            port-mirror-instance port-mirroring-instance-name;
            framing (t1 | e1);
            port port-number {
                speed (oc3-stm1 | oc12-stm4 | oc48-stm16);
            }
            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 channel-number timeslots slot-number;
                }
            }
            ct3 {
                port port-number {
                    t1 link-number {
                        channel-group channel-number timeslots slot-number;
                    }
                }
            }
            egress-policer-overhead bytes;
            framing (sdh | sonet);
            fru-poweron-sequence;
            idle-cell-format {
                itu-t;
                payload-pattern payload-pattern-byte;
            }
            ingress-policer-overhead bytes;
            linerate-mode;
            max-queues-per-interface (8 | 4);
            mlfr-uni-nni-bundles number;
            number-of-ports;
            no-concatenate;
            no-multi-rate;
            q-pic-large-buffer {
                large-scale;
                small-scale;
            }
```



```
          red-buffer-occupancy {
            weighted-averaged [ instant-usage-weight-exponent weight-value ];
          }
        sparse-dlcis;
        traffic-manager {
          egress-shaping-overhead number;
          ingress-shaping-overhead number;
          mode {
            egress-only;
            ingress-and-egress;
            session-shaping;
          }
        }
        tunnel-services {
        bandwidth (1g | 10g);
        vtmapping (itu-t | klm);
    }
}
fpc-resync;
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;
      }
      linerate-mode;
      max-queues-per-interface (8 | 4);
      no-concatenate;
      hash-key {
        family {
          inet {
            layer-3;
            layer-4;
            symmetric-hash {
              complement;
            }
          }
          multiservice {
            source-mac;
            destination-mac;
            payload {
              ip {
                layer-3;
                layer-4;
              }
            }
            symmetric-hash {
              complement;
            }
```

```
                }
              }
            }
          }
        }
        maximum-ecmp;
        offline;
        online-expected;
        sampling-instance;
      }
      memory-enhanced{
        filter;
        route;
        vpn-label;
      }
      (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;
            }
          }
        port-mirror-instance port-mirroring-instance-name;
        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 (itu-t | klm);
      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 based on a TX Matrix router or a TX Matrix Plus router. For information about a routing matrix composed of a TX Matrix router and T640 routers, see "TX Matrix Router and T640 Router Configuration Overview" on page 808 and the *TX Matrix Router Hardware Guide*. For information about a routing matrix composed of a TX Matrix Plus router and T1600 routers, see "TX Matrix Plus Router and T1600 Router Configuration Overview" on page 815 and the *TX Matrix Plus Router Hardware Guide*.

Related Documentation

- Chassis Configuration Statements

Configuring the Junos OS to Make a Flexible PIC Concentrator 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;
```

Related Documentation

- Configuring the Junos OS to Make an SFM Stay Offline on page 717
- Router Chassis Configuration Statements on page 713

Configuring the Junos OS to Make an SFM Stay Offline

By default, if you use the **request chassis sfm** CLI command to take a Switching and Forwarding Module (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.

Related Documentation

- Router Chassis Configuration Statements on page 713

Configuring the Junos OS to Resynchronize FPC Sequence Numbers with Active FPCs when an FPC Comes Online

On M320, T320, T640, T1600, TX Matrix, and TX Matrix Plus routers, when you bring a Flexible PIC Concentrator (FPC) online, the sequence number on the FPC may not be synchronized with the other active FPCs in the router, which may result in the loss of a small amount of initial traffic.

To avoid any traffic loss, include the **fpc-resync** statement at the **[edit chassis]** hierarchy level. This ensures that the sequence numbers of the FPC that is brought online is resynchronized with the other active FPCs in the router.

```
[edit chassis]
fpc-resync;
```

Related Documentation

- fpc-resync on page 846

Configuring the Junos OS for Supporting Aggregated Devices

Junos OS 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.

Tasks for configuring aggregated devices are:

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.

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 nonrevertive 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 the Junos OS to Use 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 or TX Matrix Plus router, 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;

Related Documentation

- Configuring the Junos OS to Enable ATM2 Intelligent Queuing Layer 2 Circuit Transport Mode on page 788
- Configuring the Junos OS to Support ILMI for Cell Relay Encapsulation on an ATM2 IQ PIC on page 789
- Configuring the Junos OS to Enable Idle Cell Format and Payload Patterns for ATM Devices on page 795
- **atm-cell-relay-accumulation on page 832**

Configuring Port-Mirroring Instances

Port-Mirroring Instances Overview

You can configure port mirroring for IPv4 and IPv6 traffic on all M Series, T Series, and MX Series routers. In addition, on the M7i, M10i, M120, M320, and MX Series routers, you can configure port mirroring for Layer 2 VPLS traffic.

You configure global port mirroring by including the **port-mirroring** statement at the **[edit forwarding-options]** hierarchy level. Configuring port-mirroring properties globally results in the properties being applied system-wide to all the Packet Forwarding Engines and their respective ports.

On MX Series, M320, and M120 routers, you can configure named port-mirroring instances for Layer 2 VPLS traffic. Configuring port-mirroring instances enables you to customize each instance with different properties for input-sampling and port-mirroring output destinations, instead of having to use a single system-wide configuration for port mirroring.

NOTE: **Port mirroring instances are not supported on MX80 routers. You can, however, configure port mirroring at the global level.**

You configure multiple port-mirroring instances by including the **instance** ***port-mirroring-instance-name*** statement at the **[edit forwarding-options port-mirroring]** hierarchy level. You can then associate individual port-mirroring instances with an FPC, PIC, or FEB (depending on the router).

For more information about configuring port mirroring on all routers, see the *Junos OS Routing Policy Configuration Guide*. For more information on configuring port mirroring for Layer 2 VPLS traffic on MX Series routers, see the *Junos MX Series Ethernet Services Routers Layer 2 Configuration Guide*.

Related Documentation

- Configuring Port-Mirroring Instances on MX Series 3D Universal Edge Routers on page 722
- Configuring Port-Mirroring Instances on M320 Routers on page 724
- Configuring Port-Mirroring Instances on M120 Routers on page 724

Configuring Port-Mirroring Instances on MX Series 3D Universal Edge Routers

You can configure port-mirroring instances both at the DPC level and at the PIC level on MX Series routers, as described in the following topics:

NOTE: Port mirroring instances are not supported on MX80 routers. You can, however, configure port mirroring at the global level.

- Configuring Port-Mirroring Instances at the DPC Level on page 723
- Configuring Port-Mirroring Instances at the PIC Level on page 723

Configuring Port-Mirroring Instances at the DPC Level

A port-mirroring instance configured at the FPC level for the DPC is bound to all the Packet Forwarding Engines on the DPC.

To associate a port-mirroring instance with a specific DPC and its Packet Forwarding Engines, include the **port-mirror-instance** ***port-mirroring-instance-name*** statement at the **[edit chassis fpc *slot-number*]** hierarchy level:

```
[edit chassis]
fpc slot-number {
  port-mirror-instance port-mirroring-instance-name;
}
```

The properties of the port-mirroring instance associated with the DPC override any global port-mirroring properties (configured by including the **port-mirroring** statement at the **[edit forwarding-options]** hierarchy level).

Configuring Port-Mirroring Instances at the PIC Level

For MX Series routers, there is a one-to-one mapping of Packet Forwarding Engines and PICs. Therefore, a port-mirroring instance configured at the PIC level is bound to its Packet Forwarding Engines and ports.

To associate a port-mirroring instance with a specific Packet Forwarding Engine, include the **port-mirror-instance** ***port-mirroring-instance-name*** statement at the **[edit chassis fpc *slot-number* pic *slot-number*]** hierarchy level:

```
[edit chassis]
fpc slot-number {
  port-mirror-instance port-mirroring-instance-name-a;
  pic slot-number {
    port-mirror-instance port-mirroring-instance-name-b;
  }
}
```

The properties of the port-mirroring instance associated with the PIC override the properties of the port-mirroring instance associated with the DPC (configured by including the **port-mirroring** ***port-mirroring-instance-name*** statement at the **[edit chassis fpc *slot-number*]** hierarchy level).

For more information about configuring port mirroring for Layer 2 VPLS traffic on MX Series routers, see the *Junos MX Series Ethernet Services Routers Layer 2 Configuration Guide*.

Configuring Port-Mirroring Instances on M320 Routers

You can associate only one port-mirroring instance with a specific FPC on an M320 router.

To associate a port-mirroring instance with a specific FPC, include the **port-mirror-instance** ***port-mirroring-instance-name*** statement at the **[edit chassis fpc *slot-number*]** hierarchy level:

```
[edit chassis]
fpc slot-number {
  port-mirror-instance port-mirroring-instance-name;
}
```

The properties of the port-mirroring instance associated with an FPC override any global port-mirroring properties (configured by including the **port-mirroring** statement at the **[edit forwarding-options]** hierarchy level.)

NOTE:

- Layer 2 VPLS port mirroring is supported only for Enhanced III FPCs on M320 routers.
- Ensure that the *port-mirroring-instance-name* specified at the [edit chassis fpc *slot-number*] hierarchy level matches the *port-mirroring-instance-name* configured at the [edit forwarding-options port-mirroring instance *port-mirroring-instance-name*] hierarchy level.

Related Documentation

- Port-Mirroring Instances Overview on page 722

Configuring Port-Mirroring Instances on M120 Routers

You can associate only one port-mirroring instance with a specific FEB on an M120 router.

To associate a port-mirroring instance with a FEB, include the **port-mirror-instance** ***port-mirroring-instance-name*** statement at the **[edit chassis feb *slot-number*]** hierarchy level:

```
[edit chassis]
feb slot-number {
  port-mirror-instance port-mirroring-instance-name;
}
```

The properties of the port-mirroring instance associated with the FEB override any global port-mirroring properties (configured by including the **port-mirroring** statement at the **[edit forwarding-options]** hierarchy level.)

NOTE: In a FEB redundancy group, you must associate a port-mirroring instance only with the primary FEB. During failover or switchover, the port-mirroring instance is automatically associated with the backup FEB that fails over or switches over as the primary FEB.

For information about configuring FPC-to-FEB connectivity on an M120 router, see “Configuring the Junos OS to Support FPC to FEB Connectivity on M120 Routers” on page 798.

Related Documentation

- Port-Mirroring Instances Overview on page 722

Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers

Symmetrical hashing for load balancing on an 802.3ad Link Aggregation Group (LAG) is useful when two MX Series routers (for example, Router A and Router B) are connected transparently through Deep Packet Inspection (DPI) devices over a LAG bundle. The DPI devices keep track of traffic flows in both the forward and reverse directions.

If symmetrical hashing is configured, the reverse flow of traffic is also directed through the same child link on the LAG and is bound to flow through the same DPI device. This enables proper accounting on the DPI of the traffic in both the forward and reverse flows.

If symmetrical hashing is not configured, a different child link on the LAG might be chosen for the reverse flow of traffic through a different DPI device. This results in incomplete information about the forward and reverse flows of traffic on the DPI device leading to incomplete accounting of the traffic by the DPI device.

Symmetrical hashing is computed based on fields like source address and destination address. You can configure symmetrical hashing both at the chassis level and the PIC level for load balancing based on Layer 2, Layer 3, and Layer 4 data unit fields for family inet (IPv4 protocol family) and multiservice (switch or bridge) traffic. Symmetrical hashing configured at the chassis level is applicable to the entire router, and is inherited by all its PICs and Packet Forwarding Engines. Configuring PIC-level symmetrical hashing provides you more granularity at the Packet Forwarding Engine level.

For the two routers connected through the DPI devices over a LAG bundle, you can configure **symmetric-hash** on one router and **symmetric-hash complement** on the remote-end router or vice-versa.

To configure symmetrical hashing at the chassis level, include the **symmetric-hash** or the **symmetric-hash complement** statements at the **[edit forwarding-options hash-key family]** hierarchy level. For information about configuring symmetrical hashing at the chassis level and configuring the link index, see the *Junos OS Network Interfaces Configuration Guide* and the *Junos OS VPNs Configuration Guide*.

NOTE: On MX Series DPCs, configuring symmetrical hashing at the PIC level refers to configuring symmetrical hashing at the Packet Forwarding Engine level.

To configure symmetrical hashing at the PIC level on the inbound traffic interface (where traffic enters the router), include the **symmetric-hash** or **symmetric-hash complement** statement at the [**edit chassis fpc *slot-number* pic *pic-number* hash-key**] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number hash-key]
family multiservice {
  source-mac;
  destination-mac;
  payload {
    ip {
      layer-3 (source-ip-only | destination-ip-only);
      layer-4;
    }
  }
  symmetric-hash {
    complement;
  }
}
family inet {
  layer-3;
  layer-4;
  symmetric-hash {
    complement;
  }
}
```

NOTE:

- PIC-level symmetrical hashing overrides the chassis-level symmetrical hashing configured at the **[edit chassis forwarding-options hash-key]** hierarchy level.
- Symmetrical hashing for load balancing on 802.3ad Link Aggregation Groups is currently supported for the VPLS, INET and bridged traffic only.
- Any change in the hash-key configuration requires rebooting the FPC for the changes to take effect.
- Hash key configuration on a PIC or Packet Forwarding Engine can be either in the "symmetric hash" or the "symmetric hash complement" mode, but not both at the same time.

Related Documentation

- Examples: Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs on MX Series Routers on page 727
- **family on page 841**
- **hash-key on page 848**
- **inet on page 850**
- **multiservice on page 856**
- **payload on page 862**
- **symmetric-hash on page 873**

Examples: Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs on MX Series Routers

The following examples show how to configure symmetrical hashing at the PIC level for load balancing on MX Series routers:

Configuring Symmetrical Hashing for family multiservice on Both Routers

On the inbound traffic interface where traffic enters Router A, include the **symmetric-hash** statement at the **[edit chassis fpc *slot-number* pic *pic-number* hash-key family multiservice]** hierarchy level:

```
[edit chassis fpc 2 pic 2 hash-key]
family multiservice {
  source-mac;
  destination-mac;
  payload {
    ip {
      layer-3;
      layer-4;
    }
  }
  symmetric-hash;
}
```

On the inbound traffic interface where traffic enters Router B, include the **symmetric-hash complement** statement at the **[edit chassis fpc *slot-number* pic *pic-number* hash-key family multiservice]** hierarchy level:

```
[edit chassis fpc 0 pic 3 hash-key]
family multiservice {
  source-mac;
  destination-mac;
  payload {
    ip {
      layer-3;
      layer-4;
    }
  }
  symmetric-hash {
    complement;
  }
}
```


Configuring Symmetrical Hashing for family inet on Both Routers

On the inbound traffic interface where traffic enters Router A, include the **symmetric-hash** statement at the **[edit chassis fpc *slot-number* pic *pic-number* hash-key family inet]** hierarchy level:

```
[edit chassis fpc 0 pic 1 hash-key]
family inet {
  layer-3;
  layer-4;
  symmetric-hash;
}
```

On the inbound traffic interface where traffic enters Router B, include the **symmetric-hash complement** statement at the **[edit chassis fpc *slot-number* pic *pic-number* hash-key family inet]** hierarchy level:

```
[edit chassis fpc 1 pic 2 hash-key]
family inet {
  layer-3;
  layer-4;
  symmetric-hash {
    complement;
  }
}
```

Configuring Symmetrical Hashing for family inet and family multiservice on the Two Routers

On the inbound traffic interface where traffic enters Router A, include the **symmetric-hash** statement at the **[edit chassis fpc *slot-number* pic *pic-number* hash-key family multiservice]** hierarchy level:

```
[edit chassis fpc 1 pic 0 hash-key]
family multiservice {
  payload {
    ip {
      layer-3;
      layer-4;
    }
  }
  symmetric-hash;
}
```

On the inbound traffic interface where traffic enters Router B, include the **symmetric-hash complement** statement at the **[edit chassis fpc *slot-number* pic *pic-number* hash-key family inet]** hierarchy level:

```
[edit chassis fpc 0 pic 3 hash-key]
family inet {
  layer-3;
  layer-4;
  symmetric-hash {
    complement;
  }
}
```


Related Documentation

- Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers on page 725

Configuring ECMP Next Hops for RSVP and LDP LSPs for Load Balancing

The Junos OS supports configurations of 16, 32, or 64 equal-cost multipath (ECMP) next hops for RSVP and LDP LSPs on M10i routers with an Enhanced CFEB, and M320, M120, MX Series, and T Series routers. For networks with high-volume traffic, this provides more flexibility to load-balance the traffic over as many as 64 LSPs.

To configure the maximum limit for ECMP next hops, include the **maximum-ecmp** ***next-hops*** statement at the **[edit chassis]** hierarchy level:

```
[edit chassis]
maximum-ecmp next-hops;
```

You can configure a maximum ECMP next-hop limit of **16**, **32**, or **64** using this statement. The default limit is **16**.

The following types of routes support the ECMP maximum next-hop configuration for as many as **64** ECMP gateways:

- Static IPv4 and IPv6 routes with direct and indirect next-hop ECMPs
- LDP ingress and transit routes learned through associated IGP routes
- RSVP ECMP next hops created for LSPs
- OSPF IPv4 and IPv6 route ECMPs
- ISIS IPv4 and IPv6 route ECMPs
- EBGP IPv4 and IPv6 route ECMPs
- IBGP (resolving over IGP routes) IPv4 and IPv6 route ECMPs

The enhanced ECMP limit of up to 64 ECMP next hops is also applicable for Layer 3 VPNs, Layer 2 VPNs, Layer 2 circuits, and VPLS services that resolve over an MPLS route, because the available ECMP paths in the MPLS route can also be used by such traffic.

NOTE:
The following FPCs on M320, T640, and T1600 routers only support 16 ECMP next hops:

- (M320, T640, and T1600 routers only) Enhanced II FPC1
- (M320, T640, and T1600 routers only) Enhanced II FPC2
- (M320 and T640 routers only) Enhanced II FPC3
- (T640 and T1600 routers only) FPC2
- (T640 and T1600 routers only) FPC3

If a maximum ECMP next-hop limit of 32 or 64 is configured on an M320, T640, or T1600 router with any of these FPCs installed, the Packet Forwarding Engines on these FPCs use only the first 16 ECMP next hops. For Packet Forwarding Engines on FPCs that support only 16 ECMP next hops, the Junos OS generates a system log message if a maximum ECMP next-hop limit of 32 or 64 is configured. However, for Packet Forwarding Engines on other FPCs installed on the router, a maximum configured ECMP limit of 32 or 64 ECMP next hops is applicable.

NOTE: If RSVP LSPs are configured with bandwidth allocation, for ECMP next hops with more than 16 LSPs, traffic is not distributed optimally based on bandwidths configured. Some LSPs with smaller allocated bandwidths receive more traffic than the ones configured with higher bandwidths. Traffic distribution does not strictly comply with the configured bandwidth allocation. This caveat is applicable to the following routers:

- T1600 and T640 routers with Enhanced Scaling FPC1, Enhanced Scaling FPC2, Enhanced Scaling FPC3, Enhanced Scaling FPC 4, and all Type 4 FPCs
- M320 routers with Enhanced III FPC1, Enhanced III FPC2, and Enhanced III FPC3
- MX Series routers with all types of FPCs and DPCs, excluding MPCs. This caveat is not applicable to MX Series routers with line cards based on the Junos Trio chipset.
- M120 routers with Type 1, Type 2, and Type 3 FPCs
- M10i routers with Enhanced CFEB

Next-hop cloning and permutations are disabled on T Series routers with Enhanced Scaling FPCs (Enhanced Scaling FPC1, Enhanced Scaling FPC2, Enhanced Scaling FPC3, and Enhanced Scaling FPC 4) that support enhanced load-balancing capability. As a result, memory utilization is reduced for a highly scaled system with a high number of next hops on ECMP or aggregated interfaces. Next-hop cloning and permutations are also disabled on T Series routers with Type-4 FPCs.

To view the details of the ECMP next hops, issue the **show route** command. The **show route summary command** also shows the current configuration for the maximum ECMP limit. To view details of the ECMP LDP paths, issue the **traceroute mpls ldp** command.

Related Documentation

- **maximum-ecmp on page 854**

16-Port 10-Gigabit Ethernet MPC on MX Series Routers (16x10GE 3D MPC) Overview

In Junos OS Release 10.1 and later, MX960, MX480, and MX240 routers support the 16-port 10-Gigabit Ethernet MPC (16x10GE 3D MPC) with model numbers MPC-3D-16XGE-SFPP-R-B and MPC-3D-16XGE-SFPP. This MPC provides scalability in bandwidth, subscribers, and services capabilities of the routers.

The following are some of the key features of the 16x10GE 3D MPC:

- Contains 16 built-in 10-Gigabit Ethernet ports in groups of four each. It does not contain separate slots for Modular Interface Cards (MICs).
- Supports up to 120 Gbps of full-duplex traffic.
- Supports LAN-PHY mode at 10.3125 Gbps.

NOTE: **The 16x10GE 3D MPC does not support WAN-PHY mode.**

- Supports small form-factor pluggable transceivers of the SFP+ standard. For a list of supported SFPs, see the *MX Series 3D Universal Edge Routers Line Card Guide*.
- Supports an effective line rate of twelve 10-Gigabit Ethernet ports. If all sixteen 10-Gigabit Ethernet ports are used, the line card is oversubscribed in the ratio of 4:3.
- Supports intelligent oversubscription services.
- Supports one full-duplex 10-Gigabit Ethernet tunnel interface for each Packet Forwarding Engine. For more information on configuring a full-duplex 10-Gigabit tunnel interface for this MPC, see “Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters” on page 790.

For information about the supported and unsupported Junos OS features for this MPC, see “Protocols and Applications Supported by MX Series MPCs” in the *MX Series 3D Universal Edge Routers Line Card Guide*.

Related Documentation

- 10-Gigabit Ethernet MPC with SFP+
- *MX Series 3D Universal Edge Routers Line Card Guide*.
- Configuring the Number of Active Ports on a 16-Port 10-Gigabit Ethernet MPC on MX Series Routers on page 732

- Configuring the Junos OS to Run in the IP and Ethernet Services Mode in MX Series Routers on page 805
- Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters on page 790

Configuring the Number of Active Ports on a 16-Port 10-Gigabit Ethernet MPC on MX Series Routers

The Junos OS provides the **number-of-ports *active-ports*** configuration statement at the **[edit chassis fpc *slot-number*]** hierarchy level. This statement can be used for enabling or disabling the physical ports on the Packet Forwarding Engines of a 16-port 10-Gigabit Ethernet MPC (16x10GE 3D MPC). This configuration can be used for the following purposes:

- **Enabling Switch Control Board (SCB) redundancy**—For maximum bandwidth capabilities (12-port line-rate bandwidth), the 16x10GE 3D MPC uses all the available SCBs (three SCBs for an MX960 router, two SCBs for an MX480 or MX240 router) actively in the chassis.

  If SCB redundancy (2+1 SCBs on an MX960 router or 1+1 SCB on an MX480 or MX240 router) is required, ports on the line card can be disabled by setting the number of usable ports per line card to **8**. In such a case, the third and fourth ports (ports 0/2-3, 1/2-3, 2/2-3, 3/2-3) on every Packet Forwarding Engine are disabled.
- **Ensuring guaranteed bandwidth by preventing oversubscription**—The 16x10GE 3D MPC supports one 10-Gigabit Ethernet tunnel interface for each Packet Forwarding Engine. The effective line-rate bandwidth of the MPC is 12 ports because of an oversubscription ratio of 4:3. Therefore, configuring a tunnel interface might further result in the Packet Forwarding Engines being oversubscribed. To prevent such oversubscription and to ensure a guaranteed bandwidth, include the **number-of-ports** configuration statement to disable one or two ports per Packet Forwarding Engine.

To configure the number of active ports on the MPC, include the **number-of-ports *active-ports*** configuration statement at the **[edit chassis fpc *slot-number*]** hierarchy level:

```
[edit chassis fpc slot-number]
number-of-ports (8 | 12);
```

Specify either 8 or 12 ports using this statement. When eight active ports are configured, two ports per Packet Forwarding Engine are disabled, and the LEDs on the MPC are set to **yellow**. When you specify 12 active ports, one port per Packet Forwarding Engine is disabled and the corresponding LED is set to **yellow**. When you do not include this statement in the configuration, all 16 default ports on the MPC are active.

NOTE:

- Committing the configuration after including the **number-of-ports** ***active-ports*** configuration statement brings down the Ethernet interfaces for all the ports on the MPC before the ports configuration becomes active.
- A minimum of one high-capacity fan tray is necessary for meeting the cooling requirements of the MPC. The Junos OS generates a chassis **Yellow** alarm recommending fan tray upgrade for optimal performance, if the MX router chassis contains an old fan tray.

For more information about the 16x10GE 3D MPC, see the *MX Series 3D Universal Edge Routers Line Card Guide*.

Related Documentation

- 16-Port 10-Gigabit Ethernet MPC on MX Series Routers (16x10GE 3D MPC) Overview on page 731
- Configuring the Junos OS to Run in the IP and Ethernet Services Mode in MX Series Routers on page 805
- Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters on page 790
- **number-of-ports on page 859**

Configuring Tunnel Interfaces on an MX Series Router with a 16x10GE 3D MPC

MX960, MX480, and M240 routers support the 16-port 10-Gigabit Ethernet MPC (16x10GE 3D MPC) fixed configuration Field Replaceable Unit (FRU). Each Packet Forwarding Engine on a 16x10GE MPC can support a full-duplex 10Gbps tunnel without losing line-rate capacity. For example, a full-duplex 10Gbps tunnel can be hosted on a 10-Gigabit-Ethernet port, while two other 10-Gigabit-Ethernet ports on the same PFE can concurrently forward line-rate traffic.

To configure an MPC and its corresponding Packet Forwarding Engine to use tunneling services, include the **tunnel-services** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level. The Junos OS creates tunnel interfaces **gr-*fpc/pic/port*.0**, **vt-*fpc/pic/port*.0**, and so on. You also configure the amount of bandwidth reserved for tunnel services.

```
[edit chassis]
fpc slot-number {
  pic number {
    tunnel-services {
      bandwidth 10g;
    }
  }
}
```

fpc *slot-number* is the slot number of the MPC. 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 MPC. The range is 0 through 3.

bandwidth 10g is the amount of bandwidth to reserve for tunnel traffic on each Packet Forwarding Engine.

In the following example, you create tunnel interfaces on Packet Forwarding Engine 0 of MPC 4 with 10 Gbps of bandwidth reserved for tunnel traffic. 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;
  }
}
```

Related Documentation

- 16-Port 10-Gigabit Ethernet MPC on MX Series Routers (16x10GE 3D MPC) Overview on page 731
- Configuring the Junos OS to Run in the IP and Ethernet Services Mode in MX Series Routers on page 805

Configuring the Power-On Sequence for DPCs on MX Series Routers with the Enhanced AC PEM

MX Series routers running Junos OS Release 10.0 and later support an enhanced AC Power Entry Module (PEM) to provide the necessary power infrastructure to support up to twelve higher-capacity DPCs with higher port density and slot capacity. To support the cooling requirements for the enhanced AC PEMs, the routers support enhanced fan trays and fans. The Junos OS enables you to configure the power-on sequence for the DPCs on an MX Series router chassis containing the new AC PEM. This enables you to redistribute the available power to the DPCs based on your requirements and the calculated power consumption of the DPCs. To configure the power-on sequence, include the **fru-poweron-sequence** statement at the **[edit chassis]** hierarchy level:

```
[edit chassis]
fru-poweron-sequence;
```

Issue the **show chassis power** command to view power limits and usage details for the DPCs. Issue the **show chassis power sequence** command to view details on the power-on sequence for the DPCs. For more information about these commands, see the *Junos OS System Basics and Services Command Reference*.

If the power-on sequence is not configured by including the **fru-poweron-sequence** statement, the Junos OS uses the **/var/log/poweron_seq.log** to determine the power-on sequence for the last power-on operation for the DPCs and the same sequence is used. If the **/var/log/boot_seq.log**, is not available, the Junos OS uses the ascending order of the slot numbers of the DPCs as the sequence to power-on the DPCs.

Related Documentation

- **fru-poweron-sequence on page 847**

Configuring the Junos OS to Determine the Conditions That Trigger Alarms

Configuring the Junos OS to Determine Conditions That Trigger Alarms on Different Interface Types

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 and trigger an audible alarm if one is connected. Yellow alarm conditions light the **YELLOW ALARM** LED and trigger an audible alarm if one is connected.

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.

Related Documentation

- System-Wide Alarms and Alarms for Each Interface Type on page 735
- Chassis Conditions That Trigger Alarms on page 737
- Silencing External Devices Connected to Alarm Relay Contacts on page 769

System-Wide Alarms and Alarms for Each Interface Type

Table 37 on page 736 lists the system-wide alarms and the alarms for each interface type.

Table 37: 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**

Table 37: Configurable PIC Alarm Conditions *(continued)*

Interface/System	Alarm Condition	Configuration Option
Ethernet	Link has gone down	**link-down**
DS1	Alarm indicator signal	**ais**
	Yellow alarm	**ylw**
Integrated services	Hardware or software failure	**failure**
Management Ethernet	Link has gone down	**link-down**

Related Documentation

- Configuring the Junos OS to Determine Conditions That Trigger Alarms on Different Interface Types on page 735

Chassis Conditions That Trigger Alarms

Various conditions related to the chassis components trigger yellow and red alarms. You cannot configure these conditions. Table 38 on page 737 through "Chassis Component Alarm Conditions on M5 and M10 Routers" on page 737 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 router, see the *TX Matrix Router Hardware Guide*. For information about chassis alarms for the TX Matrix Plus router, see the *TX Matrix Plus Router Hardware Guide*

Chassis Component Alarm Conditions on M5 and M10 Routers

Table 38 on page 737 lists the alarms that the chassis components can generate on M5 and M10 routers.

Table 38: Chassis Component Alarm Conditions on M5 and M10 Routers

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 **www.juniper.net/** 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

Table 38: Chassis Component Alarm Conditions on M5 and M10 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
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
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

Table 38: Chassis Component Alarm Conditions on M5 and M10 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
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
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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • Check fan.	Red
	The temperature sensor has failed.	Open a support case using the Case Manager link at **www.juniper.net/** or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Red

Chassis Component Alarm Conditions on M7i and M10i Routers

Table 39 on page 740 lists the alarms that the chassis components can generate on M7i and M10i routers.

Table 39: Chassis Component Alarm Conditions on M7i and M10i Routers

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 39: Chassis Component Alarm Conditions on M7i and M10i Routers *(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	Excessive framing errors on console port. An excessive framing error alarm is triggered when the default framing error threshold of 20 errors per second on a serial port is exceeded. This might be caused by a faulty serial console port cable connected to the device.	Replace the serial cable connected to the device. If the cable is replaced and no excessive framing errors are detected within 5 minutes from the last detected framing error, the alarm is cleared automatically.	Yellow
	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 39: Chassis Component Alarm Conditions on M7i and M10i Routers *(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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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

Chassis Component Alarm Conditions on M20 Routers

Table 40 on page 743 lists the alarms that the chassis components can generate on M20 routers.

Table 40: Chassis Component Alarm Conditions on M20 Routers

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 40: Chassis Component Alarm Conditions on M20 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Excessive framing errors on console port. An excessive framing error alarm is triggered when the default framing error threshold of 20 errors per second on a serial port is exceeded. This might be caused by a faulty serial console port cable connected to the device.	Replace the serial cable connected to the device. If the cable is replaced and no excessive framing errors are detected within 5 minutes from the last detected framing error, the alarm is cleared automatically.	Yellow
	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 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

Table 40: Chassis Component Alarm Conditions on M20 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
SSB	The control board has failed. If this occurs, the board attempts to reboot.	Replace failed control board.	Red
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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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

Chassis Component Alarm Conditions on M40 Routers

Table 41 on page 746 lists the alarms that the chassis components can generate on M40 routers.

Table 41: Chassis Component Alarm Conditions on M40 Routers

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 41: Chassis Component Alarm Conditions on M40 Routers *(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 41: Chassis Component Alarm Conditions on M40 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Excessive framing errors on console port. An excessive framing error alarm is triggered when the default framing error threshold of 20 errors per second on a serial port is exceeded. This might be caused by a faulty serial console port cable connected to the device.	Replace the serial cable connected to the device. If the cable is replaced and no excessive framing errors are detected within 5 minutes from the last detected framing error, the alarm is cleared automatically.	Yellow
	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 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 41: Chassis Component Alarm Conditions on M40 Routers *(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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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

Chassis Component Alarm Conditions on M40e and M160 Routers

Table 42 on page 749 lists the alarms that the chassis components can generate on M40e and M160 routers.

Table 42: Chassis Component Alarm Conditions on M40e and M160 Routers

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filter	Change air filter.	Change air filter.	Yellow

Table 42: Chassis Component Alarm Conditions on M40e and M160 Routers *(continued)*

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
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 42: Chassis Component Alarm Conditions on M40e and M160 Routers *(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 42: Chassis Component Alarm Conditions on M40e and M160 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Excessive framing errors on console port. An excessive framing error alarm is triggered when the default framing error threshold of 20 errors per second on a serial port is exceeded. This might be caused by a faulty serial console port cable connected to the device.	Replace the serial cable connected to the device. If the cable is replaced and no excessive framing errors are detected within 5 minutes from the last detected framing error, the alarm is cleared automatically.	Yellow
	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 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

Table 42: Chassis Component Alarm Conditions on M40e and M160 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
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 42: Chassis Component Alarm Conditions on M40e and M160 Routers *(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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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

Chassis Component Alarm Conditions on M120 Routers

Table 43 on page 754 lists the alarms that the chassis components can generate on M120 routers.

Table 43: Chassis Component Alarm Conditions on M120 Routers

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filters	Change air filter.	Change air filter.	Yellow

Table 43: Chassis Component Alarm Conditions on M120 Routers *(continued)*

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
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

Table 43: Chassis Component Alarm Conditions on M120 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
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
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

Table 43: Chassis Component Alarm Conditions on M120 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Excessive framing errors on console port. An excessive framing error alarm is triggered when the default framing error threshold of 20 errors per second on a serial port is exceeded. This might be caused by a faulty serial console port cable connected to the device.	Replace the serial cable connected to the device. If the cable is replaced and no excessive framing errors are detected within 5 minutes from the last detected framing error, the alarm is cleared automatically.	Yellow
	Error in reading or writing hard disk.	Reformat hard disk and install bootable image. If this fails, replace failed 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 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 43: Chassis Component Alarm Conditions on M120 Routers *(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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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

Chassis Component Alarm Conditions on M320 Routers

Table 44 on page 759 lists the alarms that the chassis components can generate on M320 routers.

Table 44: Chassis Component Alarm Conditions on M320 Routers

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 44: Chassis Component Alarm Conditions on M320 Routers *(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 44: Chassis Component Alarm Conditions on M320 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Excessive framing errors on console port. An excessive framing error alarm is triggered when the default framing error threshold of 20 errors per second on a serial port is exceeded. This might be caused by a faulty serial console port cable connected to the device.	Replace the serial cable connected to the device. If the cable is replaced and no excessive framing errors are detected within 5 minutes from the last detected framing error, the alarm is cleared automatically.	Yellow
	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 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
	A spare SIB is missing.	Insert spare SIB in to empty slot.	Yellow

Table 44: Chassis Component Alarm Conditions on M320 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Switch Interface Board (SIB)	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
	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. • Check air filter and replace it. • Check airflow. • Check fan.	Yellow

Table 44: Chassis Component Alarm Conditions on M320 Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature has exceeded 65 degrees C (149 degrees F), and the fans have been turned on to full speed.	• Check room temperature. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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

Chassis Component Alarm Conditions on MX Series 3D Universal Edge Routers

Table 45 on page 763 lists the alarms that the chassis components can generate on MX Series 3D Universal Edge routers.

Table 45: Chassis Component Alarm Conditions on MX Series 3D Universal Edge Routers

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filters	Change air filter.	Change air filter.	Yellow

Table 45: Chassis Component Alarm Conditions on MX Series 3D Universal Edge Routers *(continued)*

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
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
	A higher-cooling capacity fan tray is required when an MPC is installed on the chassis.	Upgrade to a high-capacity fan tray.	Yellow
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 45: Chassis Component Alarm Conditions on MX Series 3D Universal Edge Routers *(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 45: Chassis Component Alarm Conditions on MX Series 3D Universal Edge Routers *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Excessive framing errors on console port. An excessive framing error alarm is triggered when the default framing error threshold of 20 errors per second on a serial port is exceeded. This might be caused by a faulty serial console port cable connected to the device.	Replace the serial cable connected to the device. If the cable is replaced and no excessive framing errors are detected within 5 minutes from the last detected framing error, the alarm is cleared automatically.	Yellow
	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 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 45: Chassis Component Alarm Conditions on MX Series 3D Universal Edge Routers *(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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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. • Check air filter and replace it. • Check airflow. • 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

Chassis Component Alarm Conditions on TX Matrix and TX Matrix Plus Routers

For information about chassis component alarms on the TX Matrix and TX Matrix Plus routers, see the *TX Matrix Router Hardware Guide* and the *TX Matrix Plus Router Hardware Guide*, respectively.

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 46 on page 768 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 46: 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. • Reboot the system. • 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
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

Table 46: Backup Routing Engine Alarms *(continued)*

Chassis Component	Alarm Condition	Remedy	Alarm Severity
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. • 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

Related Documentation

- Configuring the Junos OS to Determine Conditions That Trigger Alarms on Different Interface Types on page 735
- Silencing External Devices Connected to Alarm Relay Contacts on page 769

Silencing External Devices Connected to Alarm Relay Contacts

You can manually silence external devices connected to alarm relay contacts. To silence an external devices, press the alarm cutoff button located on the craft interface front panel of the device.

Silencing the device does not remove the alarm messages from the display (if present on the router or switch) or extinguish the alarm LEDs. In addition, new alarms that occur after an external device is silenced reactivate the external device.

Related Documentation

- Configuring the Junos OS to Determine Conditions That Trigger Alarms on Different Interface Types on page 735
- Configuring the Junos OS to Disable the Physical Operation of the Craft Interface on page 769

Configuring the Junos OS to Disable the Physical Operation of the Craft Interface

You can disable the physical operation of the craft interface front panel on the router. When you disable 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;
```

Related Documentation

- Configuring the Junos OS to Determine Conditions That Trigger Alarms on Different Interface Types on page 735

- Silencing External Devices Connected to Alarm Relay Contacts on page 769

Configuring the Junos OS to Enable 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 router, 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.

Related Documentation

- Configuring the Junos OS to Support Layer 2 Services on MX Series 3D Universal Edge Routers with MS-DPCs on page 770

Configuring the Junos OS to Support Layer 2 Services on MX Series 3D Universal Edge Routers with MS-DPCs

The Junos OS supports Layer 2 link services on MX Series 3D Universal Edge routers with MS-DPCs and MX-FPCs with non-Ethernet IQE PICs that bundle PPP links from the Type

2 channelized SONET PICs. To enable the Layer 2 service packages such as LSQ interfaces, include the **service-package layer-2** statement at the **[edit chassis fpc *slot-number* pic *pic-number* adaptive-services]** hierarchy level:

```
[edit chassis fpc slot-number pic pic-number adaptive-services]
service-package (layer-2 | layer-3);
```

Configuring the supported link services such as Multilink PPP (MLPPP), Compressed Real-Time Transport Protocol (CRTP), real-time performance monitoring (RPM) is identical to configuring these link services for a multiservices PIC. For more information about Layer 2 link services, see the *Junos OS Services Interfaces Configuration Guide*

Related Documentation

- Configuring the Junos OS to Enable Service Packages on Adaptive Services Interfaces on page 770

Configuring the Junos OS to Enable Session Offloading on MX Series 3D Universal Edge Routers with MS-DPCs

The Junos OS enables you to configure session offloading for Multiservices DPCs on MX Series routers. This enables Fast Update Filters (FUF) at the PIC level for a multiservices interface (**ms-*fpc-pic-port***). To configure session offloading, include the **session-offload** statement at the **[edit chassis fpc *slot-number* pic *number* adaptive-services service-package extension-provider]** hierarchy level:

```
[edit chassis fpc slot-number pic number adaptive-services service-package
   extension-provider]
session-offload;
```

Currently, session offloading is supported only for a maximum of one multiservices interface.

NOTE: When session offloading is enabled for a Multiservices PIC, we recommend that you limit dynamic application awareness features for Intrusion Detection and Prevention (IDP) only for that interface.

Related Documentation

- session-offload on page 871

Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs

In Junos OS 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 routers, 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 port speed for concatenate mode on a next-generation PIC, see the *Junos OS Hardware Network Operations Guide*.

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 or TX Matrix Plus router, 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 or TX Matrix Plus router, 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;
   }
}
```

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808
- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- Configuring the Junos OS to Enable a SONET PIC to Operate in Channelized (Multiplexed) Mode on page 780

Configuring a Port Speed

Configuring a port speed allows you to enable rate-selectability on a per-port basis. When you configure a speed on a per-port basis, you can use the same MIC hardware as you upgrade your network from OC3 to OC12 or OC48 speeds.

This feature is supported on MX Series routers with SONET/SDH OC3/STM1 (Multi-Rate) MICs (MIC-3D-8OC3OC12-4OC48-SFP and MIC–3D-4OC3OC12-1OC48-SFP). By default, rate-selectability is enabled on these MICs.

To configure a port speed on the chassis for enabling rate-selectability on a per-port basis:

1. At the **[edit chassis]** hierarchy level in configuration mode, specify the port and the port speed that need to be configured. You can use one of the following speed attributes for this configuration.

   [edit chassis]
   user@host# **set fpc** ***fpc-slot*** **pic** ***pic-number*** **port** ***port-number*** **speed oc12-stm4 ;**
   user@host# **set fpc** ***fpc-slot*** **pic** ***pic-number*** **port** ***port-number*** **speed oc3-stm1 ;**
   user@host# **set fpc** ***fpc-slot*** **pic** ***pic-number*** **port** ***port-number*** **speed oc48-stm16 ;**

   For example:

   [edit chassis]
   user@host# **set fpc 3 pic 0 port 0 speed oc12-stm4**

2. Verify the configuration:

```
[edit chassis]
user@host# show
fpc 3 {
    pic 0 {
        port 0 {
              speed oc12-stm4;
           }
       }
}
```

To disable the configured rate-selectability:

1. At the **[edit chassis]** hierarchy level in configuration mode, disable rate-selectability by using the **no-multi-rate** statement.

   [edit chassis]
   user@host# **set fpc** ***fpc-slot*** **pic** ***pic-number*** **no-multi-rate**

   For example:

   [edit chassis]
   user@host# **set fpc 3 pic 0 no-multi-rate**

2. Verify the configuration:

```
[edit chassis]
user@host# show
fpc 3 {
    pic 0 {
         no-multi-rate;
           }
       }
```

NOTE: You can disable rate-selectability by using the **no-multi-rate** statement only on the 8-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP. The **no-multi-rate** statement has no effect on the 4-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, which is always rate-selectable.

Related Documentation

- **speed on page 873**
- **no-multi-rate on page 858**

Configuring the Junos OS to Support an External Clock Synchronization Interface for M Series and T Series Routers

The M320, M40e, M120, T320, T640, and T1600 routers 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.

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.

Routers that support an external clock synchronization interface include:

- M320, M40e, and M120 routers
- T320, T640, and T1600 routers

To configure external synchronization on the 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**.
- For the T320, T640, and T1600 routers, external clock interfaces are supported on the Sonic Clock Generators (SCG).
- 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, M120, and T Series routers.

- Control whether the diagnostic timing signal is transmitted.

  The **transmitter-enable** option is not available on the M120 and T Series 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 using the **primary (external-a | external-b)** statement.
- Specify the secondary external timing source using the **secondary (external-a | external-b)** statement.

Configuring an External Clock Synchronization Interface for MX Series Routers

MX80 and MX240 routers support external clock synchronization using synchronous Ethernet (SyncE). MX80T routers do not support this feature.

Configuring external clock synchronization requires making clock selection, quality level (QL), and priority considerations. The clock selection algorithm is used to pick the two best clock sources, primary and secondary, from among all the various sources, based on system configuration and execution criteria such as QL, priority, hardware restrictions, etc., and is achieved using the following logic and restrictions:

- QL must be configured for non-external clocks, whether or not QL is enabled.
- In the case of option-1, QL must be configured for external clocks (external-a or external-b), whether or not QL is enabled.
- In the case of option-2, the default QL for the external clocks is QL_STU, whether or not QL is enabled.
- Configuring priority is optional. When not specified, external-a has a higher default priority than external-b, and external-b has a higher default priority than other ge or xe clock sources, which have the lowest default priority. Configured priority is higher than any default priority.
- When QL is enabled, the received QL must be equal to or better than the configured QL for that particular source or else that source will not be considered for clock

selection. This is so that a downstream client is guaranteed clock quality of a certain level (that 'certain level' being the configured QL).

- During clock selection:
  - The active source with highest QL is selected.
  - If QL is the same for two or more sources, then the source with highest priority wins.
  - If two or more sources have the same QL and priority, then currently active source, if any, among these sources wins.
  - If two or more sources have the same QL and priority, and none of these is currently active, then any one of these may be picked.
  - The configured (or default) QL of the selected clock source is used for Ethernet Synchronization Messaging Channel (ESMC).
  - If the primary clock source is ge|xe-x/y/z, where y is even (0 or 2), then the secondary cannot be ge|xe-/x/y/* or ge|xe-/x/y + 1/*. E.g., if ge-1/2/3 is the primary clock source, then the secondary cannot be ge-1/2/* or ge-1/3/* for an MX80 or MX240 router.
  - If the primary clock source is ge|xe-x/y/z, where y is odd (1 or 3), then the secondary cannot be ge|xe-/x/y/* or ge|xe-/x/y - 1/*. E.g., if xe-2/3/4 is the primary, then the secondary cannot be xe-2/2/* or xe-2/3/* for an MX80 or MX240 router.
  - If the primary clock source is ge|xe-x/y/z, then the secondary cannot be ge|xe-x/y/* in the case of 12-16x10G DPC on an MX Series router e.g., if ge-/0/1/2, is primary, then ge-0/1/* cannot be the secondary clock source, but ge-/0/0/* may be the secondary.

Setting the clock type

To set the clock type, use the following command:

```
set chassis synchronization network-type (option-1 | option-2)
```

EEC-1 maps to G.813 option 1 and EEC-2 maps to G.812 type IV clock.

Setting the clock mode

To set the mode of operation to select the clock source either from free-run local oscillator or from an external qualified clock, use the following command:

```
set chassis synchronization clock-mode (free-run | auto-select)
```

For MX80 routers, the free-run clock is provided by the SCB.

For MX240 routers, the free-run clock is provided by the local oscillator.

The default for both routers is auto-select mode.

Setting the quality mode

To set the synchronization quality mode, use the following command:

```
set chassis synchronization quality-mode-enable
```

The default is disable.

Setting the switchover, config-change, or reboot times

To set the switchover, configuration-change, or restart time, use the following command:

```
set chassis synchronization hold-interval (configuration-change | restart |
switchover) seconds
```

This sets the time interval to wait before selecting the new clock source during.

The default switchover time is 30 seconds and cold boot time is 120 seconds.

Setting the synchronization switching mode

To set the synchronization switchover mode, use the following command:

```
set chassis synchronization switchover-mode (revertive | non-revertive)
```

In revertive mode, the system will switch from a lower to a higher quality clock source whenever the higher clock source becomes available.

In non-revertive mode, the system will continue use the current clock source as long as it is valid.

The default mode is revertive.

Setting the clock source

To set the clock source, use the following command:

```
set chassis synchronization source (external-a | external-b | interfaces
interface-name)
```

The clock source is specified using the clock selection process.

Setting ESMC packet transmit

- To enable ESMC packet transmit, use the following command:

```
set chassis synchronization esmc-transmit interfaces interface-name
```

Setting the synchronization source quality level

To set the synchronization source quality level, use the following command:

```
set chassis synchronization source (external-a | external-b | interfaces
interface-name) quality-level (prc | prs |sec | smc | ssu-a | ssu-b | st2 | st3 |
st3e | st4 | stu | tnc)
```

Both option I and option II SSM quality levels are supported.

The quality level is set to DNU for network-option 1 and set to DUS for network-option 2, if quality-level not configured and no ESMC messages received.

On selected active source (primary or secondary which is active), even if ESMC transmit is not enabled, a DNU ESMC will be sent out if network-option is 1, and DUS ESMC will be sent out if network-option is 2. This is applicable only for Ethernet interface type sources. This is done to avoid the source looping, as per the standard requirement.

Setting the synchronization source priority

To set the synchronization source priority, use the following command:

```
set chassis synchronization source (external-a | external-b | interfaces
interface-name) priority number
```

Setting the synchronization source wait to restore time

To set the synchronization source wait to restore time, use the following command:

```
set chassis synchronization source interfaces interface-name wait-to-restore
minutes
```

A wait-to-restore time can be configured for each port. When a port's signal transitions out of the signal fail state it must be fault free for the wait-to-restore time before it is again considered by the selection process.

The range is 0 to 12 minutes.

The default time is 5 minutes.

Setting the synchronization source lockout

To set the synchronization source lockout, use the following command:

```
set chassis synchronization source (external-A | external-B | interfaces
interface-name) request lockout
```

Lockout may be configured for any source. When configured, that source will not be considered by the selection process.

Setting the forced switch

To set the forced switch, use the following command:

```
set chassis synchronization source (external-A | external-B | interfaces
interface-name) request force-switch
```

Forces a switch to the source provided the source is enabled and not locked out. Only one configured source may be force-switched.

Related Documentation

- request chassis synchronization mode
- **synchronization (MX Series) on page 876**

Configuring the Junos OS to Support the Sparse DLCI Mode on Channelized STM1 or Channelized DS3 PICs

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.

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;
```

Related Documentation

- Configuring the Junos OS to Enable a SONET PIC to Operate in Channelized (Multiplexed) Mode on page 780
- Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots on page 781
- Configuring the Junos OS to Support Channel Groups and Time Slots for Channelized E1 PICs on page 785
- Configuring the Junos OS to Support Channelized STM1 Interface Virtual Tributary Mapping on page 787
- Configuring the Junos OS to Enable Larger Delay Buffers for T1, E1, and DS0 Interfaces Configured on Channelized IQ PICs on page 801

Configuring the Junos OS to Enable a SONET PIC to Operate in Channelized (Multiplexed) Mode

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 or TX Matrix Plus router, 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**.

NOTE: 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 4-port SONET/SDH OC3 PIC cannot run in nonconcatenated mode on any platform.

Related Documentation

- Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs on page 772
- Configuring the Junos OS to Support the Sparse DLCI Mode on Channelized STM1 or Channelized DS3 PICs on page 779

Configuring Channelized DS3-to-DS0 Naming

Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots

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 47 on page 783 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 *channel-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.

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 in this example:

[edit chassis fpc 0 pic 1 ct3 port 5 t1 22]
channel-group 7 timeslots 1-10;

To use time slots 1 through 5, time slot 10, and time slot 24, designate ***slot-number*** as in this example:

[edit chassis fpc 2 pic *pic-number*1 ct3 port 0 t1 8]
channel-group 4 timeslots 1-5,10,24;

Do not include spaces in the list of time slot numbers.

Related Documentation

- Ranges for Channelized DS3-to-DS0 Configuration on page 782

Ranges for Channelized DS3-to-DS0 Configuration

Table 47 on page 783 shows the ranges for each of the quantities in the preceding configuration.

Table 47: 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

Related Documentation

- Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots on page 781

Configuring the Junos OS to Support Eight Queues on IQ Interfaces for T Series and M320 Routers

By default, IQ PICs on T Series and M320 routers 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 or TX Matrix Plus router, 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 routers, 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.

Related Documentation

- Configuring the Junos OS to Support ILMI for Cell Relay Encapsulation on an ATM2 IQ PIC on page 789
- Configuring the Junos OS to Enable Larger Delay Buffers for T1, E1, and DS0 Interfaces Configured on Channelized IQ PICs on page 801

Configuring a Policer Overhead

Configuring a policer overhead allows you to control the rate of traffic sent or received on an interface. When you configure a policer overhead, the configured policer overhead value (bytes) is added to the length of the final Ethernet frame. This calculated length of frame is used to determine the policer or the rate limit action. Therefore, the policer overhead enables you to control the rate of traffic sent or received on an interface. You can configure the policer overhead to rate-limit queues and Layer 2 and MAC policers. The policer overhead and the shaping overhead can be configured simultaneously on an interface.

This feature is supported on M Series and T Series routers with IQ2 PICs or IQ2E PICs, and on MX Series DPCs.

To configure a policer overhead for controlling the rate of traffic sent or received on an interface:

1. In the **[edit chassis]** hierarchy level in configuration mode, create the interface on which to add the policer overhead to input or output traffic.

   [edit chassis]
   user@host# **edit fpc *fpc* pic *pic***

   For example:

   [edit chassis]
   user@host# **edit fpc 0 pic 1**

2. Configure the policer overhead to control the input or output traffic on the interface. You could use either statement or both the statements for this configuration.

   [edit chassis fpc *fpc* pic *pic*]
   user@host# **set ingress-policer-overhead *bytes*;**
   user@host# **set egress-policer-overhead *bytes*;**

For example:

[edit chassis fpc 0 pic 1]
user@host# **set ingress-policer-overhead** 10;
user@host# **set egress-policer-overhead** 20;

3. Verify the configuration:

```
[edit chassis]
user@host# show
fpc 0 {
    pic 1 {
        ingress-policer-overhead 10;
        egress-policer-overhead 20;
    }
}
```

NOTE: When the configuration for the policer overhead bytes on a PIC is changed, the PIC goes offline and then comes back online. In addition, the configuration in the CLI is on a per-PIC basis and, therefore, applies to all the ports on the PIC.

Related Documentation

- **egress-policer-overhead on page 840**
- **ingress-policer-overhead on page 851**

Configuring Channel Groups and Time Slots for a Channelized E1 Interface

Configuring the Junos OS to Support Channel Groups and Time Slots for Channelized E1 PICs

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 48 on page 787 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 channel-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.

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 in this example:

```
[edit chassis fpc 1 pic 2 ce1 e1 6]
channel-group 3 timeslots 1-10;
```

To use time slots 1 through 5, time slot 10, and time slot 24, designate ***slot-number*** as in this example:

```
[edit chassis fpc 3 pic 0 ce1 e1 2]
channel-group 1 timeslots 1-5,10,24;
```

Do not include spaces in a list of time slot numbers.

For further information about these interfaces, see the *Junos Network Interfaces Configuration Guide*.

Related Documentation

- Ranges for Channelized E1 Interfaces Configuration on page 787

Ranges for Channelized E1 Interfaces Configuration

Table 48 on page 787 shows the ranges for configuring channel groups and time slots for Channelized E1 Interfaces.

Table 48: 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
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 router. For the TX Matrix and TX Matrix Plus routers, the range is from 0 through 31. For M40, M40e, M160, M320, M120, and other T Series routers, the range is from 0 through 7. For M20 routers, the range is from 0 through 3. For M10 and M10i routers, the range is from 0 through 1. For M5 and M7i routers, the only applicable value is 0.

Related Documentation

- Configuring the Junos OS to Support Channel Groups and Time Slots for Channelized E1 PICs on page 785

Configuring the Junos OS to Support 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.

Related Documentation

- Configuring the Junos OS to Support the Sparse DLCI Mode on Channelized STM1 or Channelized DS3 PICs on page 779

Configuring the Junos OS to Enable 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 or TX Matrix Plus router, 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.**

Related Documentation

- Configuring the Junos OS to Support ILMI for Cell Relay Encapsulation on an ATM2 IQ PIC on page 789
- Configuring the Junos OS to Enable Idle Cell Format and Payload Patterns for ATM Devices on page 795
- Configuring the Junos OS to Use ATM Cell-Relay Accumulation Mode on an ATM1 PIC on page 721

Configuring the Junos OS to Support ILMI for Cell Relay Encapsulation on an ATM2 IQ PIC

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*.

Related Documentation

- Configuring the Junos OS to Enable ATM2 Intelligent Queuing Layer 2 Circuit Transport Mode on page 788

Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters

Because the MX Series routers do not support Tunnel Services PICs, you create tunnel interfaces on MX Series routers by including 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, MPC, or MIC. On the MX80 router, the range is 0 through 1.On other MX series routers, 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.

The **pic *number*** On MX80 routers, if the FPC is 0, the PIC number can only be 0. If the FPC is 1, the PIC range is 0 through 3. For all other MX series routers, 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.

10g indicates that 10 Gbps of bandwidth is reserved for tunnel traffic.

If you specify a bandwidth that is not compatible, 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.

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*.

Related Documentation

- Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC on page 790
- Example: Configuring Tunnel Interfaces on a 10-Gigabit Ethernet 4-Port DPC on page 791

Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC

The following example shows how to 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 {
        bandwidth 1g;
    }
}
```

Related Documentation

- Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters on page 790
- Configuring the Junos OS to Support ILMI for Cell Relay Encapsulation on an ATM2 IQ PIC on page 789

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;
    }
}
```

Related Documentation

- Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters on page 790
- Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC on page 790

Configuring the Junos OS to Enable an M160 Router to Operate in Packet Scheduling Mode

By default, packet scheduling is disabled on M160 Routers. 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 Junos OS to Allocate More Memory for Routing Tables, Firewall Filters, and Layer 3 VPN Labels

The jtree memory on all MX Series, all M120, and some M320, M10i, M7i, T640, T1600, TX Matrix, and TX Matrix Plus router Packet Forwarding Engines has two segments: one segment primarily stores routing tables and related information, and the other segment primarily stores firewall-filter-related information.

The Junos OS provides the **memory-enhanced** statement to reallocate the jtree memory for routes, firewall filters, and Layer 3 VPNs. The statement has the following options:

- **filter**—Include this statement when you want to support larger firewall filters over routing tables. However, we recommend enabling this option only if you do not have a very large routing table configuration.

  To allocate more memory for firewall filters, include the **filter** statement at the **[edit chassis memory-enhanced]** hierarchy level:

  ```
  [edit chassis memory-enhanced]
  filter;
  ```

- **route**—Include this statement when you want to support larger routing tables (with more routes) over firewall filters. For example, you can enable this option, when you want to support a large number of routes for Layer 3 VPNs implemented using MPLS. However, we recommend enabling this option only if you do not have a very large firewall configuration.

  To allocate more memory for routing tables, include the **route** statement at the **[edit chassis memory-enhanced]** hierarchy level:

  ```
  [edit chassis memory-enhanced]
  route;
  ```

- **vpn-label**—Include this statement when you want to enhance memory to support a larger number of Layer 3 VPN labels.

  Layer 3 VPN composite next hops can be enabled by including the **l3vpn-composite-nexthop** statement at the **[edit routing-options]** and **[edit logical-systems *logical-system-name* routing-options]** hierarchy levels. This statement enables BGP to accept larger numbers of Layer 3 VPN BGP updates with unique inner VPN labels. Including the **l3vpn-composite-nexthop** in the configuration enhances scaling and convergence performance of PE routers participating in a Layer 3 VPN in a multivendor environment. For more information on configuring the **l3vpn-composite-nexthop** statement, see the *Junos OS VPNs Configuration Guide*.

To allocate more memory to support a larger number of Layer 3 VPN labels accepted by the **l3vpn-composite-nexhop** statement, include the **vpn-label** statement at the **[edit chassis memory-enhanced]** hierarchy level:

```
[edit chassis memory-enhanced]
vpn-label;
```

You can configure the **memory-enhanced** statement on the following routers:

- M10i and M7i routers with Enhanced CFEB
- M320 routers with Enhanced III FPC1, Enhanced III FPC2, and Enhanced III FPC3
- M120 routers
- MX Series routers
- T Series (T640, T1600, TX Matrix, and TX Matrix Plus) routers with Enhanced Scaling FPC1, Enhanced Scaling FPC2, Enhanced Scaling FPC3, and Enhanced Scaling FPC4.

As the allocation of more memory for routing tables or firewall filters might disrupt the forwarding operations of a Packet Forwarding Engine, the Junos OS CLI displays a warning to restart all affected FPCs when you commit a configuration that includes the **memory-enhanced** statement. The configuration does not become effective until you restart the FPC or DPC (on MX Series routers).

To restart a single FPC or DPC without rebooting the entire router, issue the **request chassis fpc slot *slot-number* restart** command. On an M120 router, issue the **request chassis feb slot *slot-number* restart** command.

To view if the configuration is active on an FPC or DPC, issue the **show pfe fpc *slot-number*** command.

NOTE:

- For T Series routers only. With Junos OS Release 10.2, enhanced jtree memory allocation is disabled by default. For Junos OS Releases 9.3 through 10.1, the default routing tables (**inet.0** and **inet6.0**) use both memory segments by default.
- In Junos OS Release 11.2 and later, the **memory-enhanced route** statement at the **[edit chassis]** hierarchy level replaces the **route-memory-enhanced** statement at the **[edit chassis]** hierarchy level.
- The **filter** statement is supported only on T Series routers.

Related Documentation

- **memory-enhanced on page 855**
- **filter on page 842**
- **route on page 868**
- **vpn-label on page 884**

Configuring the Link Services PIC for Multilink Protocol Support

Configuring the Junos OS to Support the Link Services PIC

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 Link 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.

NOTE: **The Link Services PIC is not compatible with the M160 or T Series routers.**

Related Documentation

- Multiclass Extension for Multiple Classes of Service Using MLPPP (RFC 2686) on page 795

Multiclass Extension for Multiple Classes of Service Using MLPPP (RFC 2686)

The multiclass extension to the MLPPP extension enables multiple classes of service using MLPPP. For more information, see RFC 2686, *The Multi-Class Extension to Multi-Link PPP*. The Junos OS PPP implementation does not support the negotiation of address field compression and protocol field compression PPP NCP options. The software always sends a full 4-byte PPP header.

Related Documentation

- Configuring the Junos OS to Support the Link Services PIC on page 794

Configuring the Junos OS to Enable Idle Cell Format and Payload Patterns for ATM Devices

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 or TX Matrix Plus router, 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 router, 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 router, see "TX Matrix Router and T640 Router Configuration Overview" on page 808. For information about the TX Matrix Plus router, see "TX Matrix Plus Router and T1600 Router Configuration Overview" on page 815.

Related Documentation

- Configuring the Junos OS to Use ATM Cell-Relay Accumulation Mode on an ATM1 PIC on page 721
- Configuring the Junos OS to Enable ATM2 Intelligent Queuing Layer 2 Circuit Transport Mode on page 788
- Configuring the Junos OS to Support ILMI for Cell Relay Encapsulation on an ATM2 IQ PIC on page 789

Configuring the Junos OS to Enable MTU Path Check for a Routing Instance on M Series Routers

By default, the maximum transmission unit (MTU) check for routing instance is disabled on M Series routers (except the M120 and M320 routers), 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 M120 and M320 routers) 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 router 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, complete the following tasks:

1. Enabling MTU Check for a Routing Instance on page 796
2. Assigning an IP Address to an Interface in the Routing Instance on page 796

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.

Configuring the Junos OS to Support Redundancy on Routers Having Multiple Routing Engines or Switching Boards

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.

To configure redundancy, include the following redundancy statements 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);
}
```

Related Documentation

- Understanding Routing Engine Redundancy on Juniper Networks Routers

Configuring the Junos OS to Support 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.

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;
}
```

Related Documentation

- Configuring the Junos OS to Support an External Clock Synchronization Interface for M Series and T Series Routers on page 775
- Configuring Port-Mirroring Instances on M120 Routers on page 724

Configuring the Junos OS to Enable a Routing Engine to Reboot 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 recover from this situation, you can configure a single Routing Engine to reboot automatically when a hard disk error occurs. To enable this feature, include the **on-disk-failure reboot** statement at the **[edit chassis routing-engine]** hierarchy level.

```
[edit chassis routing-engine]
```



```
on-disk-failure {
  disk-failure-action (halt | reboot);
}
```

For dual Routing Engine environments, you can configure a backup Routing Engine to assume mastership automatically, if 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 OS High Availability Configuration Guide*.

You can configure the Routing Engine to halt (instead of rebooting) when the hard disk fails on the Routing Engine. To configure this feature, 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 the **halt** option to configure the Routing Engine to halt when the hard disk fails. Use the **reboot** option to configure the Routing Engine to reboot when the hard disk fails.

Related Documentation

- Configuring Automatic Mirroring of the CompactFlash Card on the Hard Disk Drive on page 68

Configuring the Junos OS to Prevent the Resetting of the Factory Default or Rescue Configuration During Current Configuration Failure on J Series Routers

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 to Prevent Congestion And Packet Dropping

Configuring the Junos OS to Enable Larger Delay Buffers for T1, E1, and DS0 Interfaces Configured on Channelized IQ PICs

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. To set the average packet size used to calculate the number of notification queue entries in the IQ PIC to 256 bytes, 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;
}
```

On a TX Matrix router or a TX Matrix Plus router, include the **q-pic-large-buffer large-scale** 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]
q-pic-large-buffer {
  large-scale;
}
```

NOTE: When you commit the configuration after including the **q-pic-large-buffer** statement for a PIC, the Junos OS temporarily takes the PIC offline and brings it back online before the new configuration is activated and becomes the current operational configuration.

This statement sets the maximum buffer size. (See Table 49 on page 802.)

For information on configuring the buffer size, see the *Junos Class of Service Configuration Guide*.

Related Documentation

- Maximum Delay Buffer with q-pic-large-buffer Statement Enabled on page 802

Maximum Delay Buffer with q-pic-large-buffer Statement Enabled

Table 49 on page 802 lists the maximum delay buffer that can be configured for T1, E1, and DS0 interfaces configured on Channelized IQ PICs:

Table 49: 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 routers	50,000 microseconds
Other M Series routers	200,000 microseconds
IQ PICs on all routers	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
With shaping rate from 30,000,001 bps through 40 Mbps	150,000 microseconds

Table 49: Maximum Delay Buffer with q-pic-large-buffer Statement Enabled *(continued)*

Platform, PIC, or Interface Type	Maximum Buffer Size
With shaping rate up to 40,000,001 bps or higher	100,000 microseconds
*N*xDS0 IQ Interfaces—Maximum sizes vary by channel size:	
1xDS0 through 3xDS0	4,000,000 microseconds
4xDS0 through 7xDS0	2,000,000 microseconds
8xDS0 through 15xDS0	1,000,000 microseconds
16xDS0 through 32xDS0	500,000 microseconds
Other IQ interfaces	500,000 microseconds

Related Documentation

- Configuring the Junos OS to Enable Larger Delay Buffers for T1, E1, and DS0 Interfaces Configured on Channelized IQ PICs on page 801

Configuring the Junos OS to Support Entry-Level Configuration on an M320 Router with a Minimum Number of SIBs and PIMs

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.

Related Documentation

- Configuring Port-Mirroring Instances on M320 Routers on page 724
- Configuring the Junos OS to Support an External Clock Synchronization Interface for M Series and T Series Routers on page 775
- Configuring the Junos OS to Support Eight Queues on IQ Interfaces for T Series and M320 Routers on page 783

Configuring the uPIM to Run in Switching or Routing Mode on J Series Routers

Configuring the Junos OS to Support 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);
    }
  }
}
```

Related Documentation

- Configuring the Junos OS to Set a PIM Offline on J Series Routers on page 804
- Configuring the Junos OS to Disable Power Management on the J Series Chassis on page 805

Configuring the Junos OS to Set a PIM Offline on J Series Routers

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;
```


Related Documentation

- Configuring the Junos OS to Support the uPIM Mode on J Series Routers on page 804
- Configuring the Junos OS to Disable Power Management on the J Series Chassis on page 805

Configuring the Junos OS to Disable 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 because of 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;
```

Related Documentation

- Configuring the Junos OS to Set a PIM Offline on J Series Routers on page 804
- Configuring the Junos OS to Support the uPIM Mode on J Series Routers on page 804

Configuring the IP and Ethernet Services Mode in MX Series Routers

Configuring the Junos OS to Run in the IP and Ethernet Services Mode in MX Series Routers

MX Series 3D Universal Edge Routers can be configured to run in IP Services mode or Ethernet Services mode. The default IP Services mode provides complete functionality. 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 50 on page 806.

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);
```

- A router chassis with a 16x10GE MPC with model number MPC-3D-16XGE-SFPP requires that the chassis be configured in the Ethernet network services mode.
- A router chassis with a 16x10GE MPC with model number MPC-3D-16XGE-SFPP-R-B can be configured in the Ethernet network services mode or the IP network services mode. However, this requires installing the appropriate license to enable the use of the IP network services mode.
- A router chassis with both 16x10GE MPC models, MPC-3D-16XGE-SFPP and MPC-3D-16XGE-SFPP-R-B must be configured in the Ethernet network services mode.

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.

Related Documentation

- Restrictions on Junos Features for MX Series Routers on page 806
- 16-Port 10-Gigabit Ethernet MPC on MX Series Routers (16x10GE 3D MPC) Overview on page 731

Restrictions on Junos Features for MX Series Routers

The following features contain restrictions when running in Ethernet Services mode.

Table 50: 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. • Data plane support applies only for Ethernet and MPLS. • 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 in Ethernet Services mode.
Source and destination class usage (SCU and DCU)	Source and Destination Class Usage is disabled in Ethernet Services mode.
Filter terms	In Ethernet Services mode, the number of externally configured filter terms is restricted to 64 KB.

Related Documentation

- Configuring the Junos OS to Run in the IP and Ethernet Services Mode in MX Series Routers on page 805

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** statement at the **[edit interfaces ge-*pim*/0/0 switch-options]** hierarchy level:

```
[edit interfaces ge-pim /0/0 switch-options]
switch-port port-number {
  (auto-negotiation | no-auto-negotiation);
  speed (10m | 100m | 1g);
  link-mode (full-duplex | half-duplex);
}
```

Related Documentation

- Example: Configuring J Series Services Router Switching Interfaces on page 807

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;
    }
  }
}
```

Related Documentation

- Configuring J Series Services Router Switching Interfaces on page 806

TX Matrix Router and T640 Router Configuration Guidelines

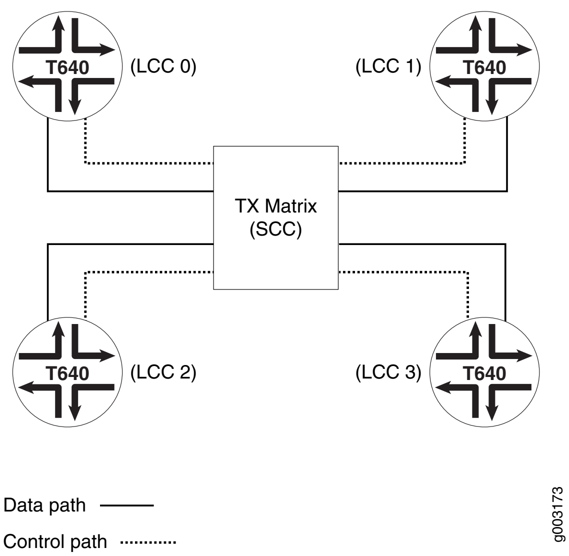
TX Matrix Router and T640 Router Configuration Overview

This topic provides an overview of configuring the TX Matrix router and T640 routers.

TX Matrix Router and T640 Router-Based Routing Matrix Overview

A routing matrix is a multichassis architecture that consists of a TX Matrix router and from one to four T640 routers. From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix router controls all the T640 routers in the routing matrix, as shown in Figure 11 on page 808.

Figure 11: Routing Matrix Composed of a TX Matrix Router and Four T640 Routers



You configure and manage the TX Matrix router and its T640 routers in the routing matrix through the CLI on the TX Matrix router. This means that the configuration file on the TX Matrix router is used for the entire routing matrix.

Because all configuration, troubleshooting, and monitoring are performed through the TX Matrix router, we do not recommend accessing its T640 routers 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 router:

```
% 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 router is not propagated to the TX Matrix router or other T640 routers in the routing matrix. For details, see "Committing Configurations on the TX Matrix Router" on page 809.

Running Different Junos OS Releases on the TX Matrix Router and T640 Routers

On a routing matrix, if you elect to run different Junos OS Releases on the TX Matrix router and T640 Routing Engines, a change in Routing Engine mastership can cause one or all T640 routers to be logically disconnected from the TX Matrix router.

NOTE: The routing matrix supports Release 7.0 and later versions of the Junos OS. 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 Router Hardware Guide*.

TX Matrix Router Software Upgrades and Reinstallation

By default, when you upgrade or reinstall software on the TX Matrix router, the new software image is distributed to the connected T640 routers. Software installed on a primary TX Matrix router is distributed to all connected primary T640 routers and the backup is distributed to all connected backup routers.

TX Matrix Router Rebooting Process

When you reboot the TX Matrix router master Routing Engine, all the master Routing Engines in the connected T640 routers reboot. In addition, you can selectively reboot the master Routing Engine or any of the connected T640 routers.

Committing Configurations on the TX Matrix Router

In a routing matrix composed of a TX Matrix router and T640 routers, all configuration must be performed on the TX Matrix router. Any configuration you commit on a T640 router is not propagated to the TX Matrix router or other T640 routers. Only configuration changes you commit on the TX Matrix router are propagated to all T640 routers. A commit on a TX Matrix router overrides any changes you commit on a T640 router.

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 router.

If you issue the **commit synchronize** command on the TX Matrix router, 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
```

TX Matrix and T640 Router 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 router. In addition, the routing matrix supports group names for the Routing Engines for each T640 router: **lcc *n*-re0** and **lcc *n*-re1**. ***n*** identifies a T640 router from 0 through 3.

Routing Matrix System Log Messages

You configure the T640 routers to forward their system log messages to the TX Matrix router at the **[edit system syslog host scc-master]** hierarchy level. For information about how to configure system log messages in a routing matrix, see "Junos OS System Log Configuration Overview" on page 139 and "Configuring System Logging for a TX Matrix Router" on page 167.

Related Documentation

- Using the Junos OS to Configure a T640 Router Within a Routing Matrix on page 810

Using the Junos OS to Configure a T640 Router Within a Routing Matrix

A routing matrix composed of a TX Matrix router and T640 routers supports the same chassis configuration statements as a standalone router (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 routers. In addition, a routing matrix has two more chassis configuration statements, **online-expected** and **offline**.

To configure a T640 router that is connected to a TX Matrix router, include the **lcc** statement at the **[edit chassis]** hierarchy level:

```
[edit chassis]
lcc number;
```

number can be 0 through 3.

To configure a T640 router 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;
q-pic-large-buffer {
  large-scale;
}
```

NOTE: For the FPC slot number, specify the actual hardware slot number (numbered 0 through 7) as labeled on the T640 router chassis. Do not use the corresponding software FPC number shown in Table 51 on page 812.

For information about how to configure the **online-expected** and **offline** configuration statements, see "Configuring the Junos OS to Enable the TX Matrix Router to Generate an Alarm If a T640 Router Stays Offline" on page 814.

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808
- TX Matrix Router Chassis and Interface Names on page 811
- Configuring the Junos OS to Upgrade and Downgrade Switch Interface Boards on a TX Matrix Router on page 813
- Configuring the Junos OS to Enable the TX Matrix Router to Generate an Alarm If a T640 Router Stays Offline on page 814

TX Matrix Router 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 router. Similarly the terms LCC, and **lcc** as a prefix (for *line-card chassis*) refer to a T640 router in a routing matrix.

T640 routers are assigned LCC index numbers, 0 through 3, depending on the hardware setup of the routing matrix. A routing matrix can have up to four T640 routers, and each T640 router 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 OS CLI, an interface name has the following format:

type-*fpc*/*pic*/*port*

When you specify the FPC number, the Junos OS determines which T640 router 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 routers to the correct FPC in a routing matrix, use the conversion chart shown in Table 51 on page 812. You can use the converted FPC number to configure the interfaces on the TX Matrix router in your routing matrix.

Table 51: T640 to Routing Matrix FPC Conversion Chart

FPC Numbering	T640 Routers							
	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
	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

Table 51: T640 to Routing Matrix FPC Conversion Chart *(continued)*

FPC Numbering	T640 Routers							
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 router **LCC 3**, you can configure this interface on the TX Matrix router 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;
      }
    }
  }
}
```

Related Documentation

- Using the Junos OS to Configure a T640 Router Within a Routing Matrix on page 810

Configuring the Junos OS to Upgrade and Downgrade Switch Interface Boards on a TX Matrix Router

The Junos OS 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.

Configuring the Junos OS to Upgrade Switch Interface Boards on a TX Matrix Router

To configure the TX Matrix router 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 router are propagated to all T640 routers in a routing matrix.

```
[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.

Configuring the Junos OS to Downgrade Switch Interface Boards on a TX Matrix Router

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.

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808
- Using the Junos OS to Configure a T640 Router Within a Routing Matrix on page 810

Configuring the Junos OS to Enable the TX Matrix Router to Generate an Alarm If a T640 Router Stays Offline

By default, the Junos OS enables all the T640 routers in the routing matrix to come online. The Junos OS also allows you to configure all the T640 routers so that if they do not come online, an alarm is sent by the TX Matrix router.

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 router 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 router. When the T640 router is ready to come back online, delete the **offline** configuration statement.

To configure a T640 router 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 router that is part of the routing matrix is allowed to come online. However, if a T640 router does not come online, the TX Matrix router does not generate an alarm.**

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808
- Using the Junos OS to Configure a T640 Router Within a Routing Matrix on page 810

TX Matrix Plus Router and T1600 Router Configuration Guidelines

TX Matrix Plus Router and T1600 Router Configuration Overview

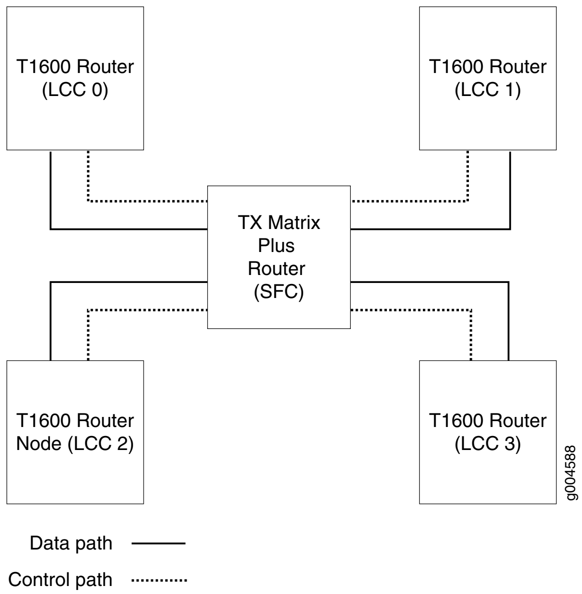
This topic provides an overview of configuring the TX Matrix Plus router and T1600 routers.

TX Matrix Plus Router and T1600 Router-Based Routing Matrix Overview

A routing matrix based on a TX Matrix Plus router is a multichassis architecture that consists of a TX Matrix Plus router and from one to four T1600 routers. From the perspective of the user interface, the routing matrix appears as a single router. The TX

Matrix Plus router (or switch-fabric chassis (SFC)) controls all the T1600 routers (or line-card chassis (LCC)) in the routing matrix, as shown in Figure 12 on page 816.

Figure 12: Routing Matrix Composed of a TX Matrix Plus Router and Four T1600 Routers



You configure and manage the TX Matrix Plus router and its T1600 routers in the routing matrix through the CLI on the TX Matrix Plus router. This means that the configuration file on the TX Matrix Plus router is used for the entire routing matrix.

Because all configuration, troubleshooting, and monitoring are performed through the TX Matrix Plus router, we do not recommend accessing its T1600 routers directly (through the console port or management Ethernet interface [**em0**]). If you do, the following messages appear when you first start the CLI through a T1600 router:

```
% 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 Fabric Chassis (SFC).
warning: Please logout and log into the SFC to use CLI.
```

These messages appear because any configuration you commit on a T1600 router is not propagated to the TX Matrix Plus router or other T1600 routers in the routing matrix. For details, see "Committing Configurations on the TX Matrix Plus Router" on page 818.

Running Different Junos OS Releases on the TX Matrix Plus Router and T1600 Routers

On a routing matrix composed of a TX Matrix Plus router and T1600 routers, if you elect to run different Junos OS Releases on the TX Matrix Plus router and T1600 Routing Engines, a change in Routing Engine mastership can cause one or all T1600 routers to be logically disconnected from the TX Matrix Plus router.

NOTE: All the master Routing Engines on the routing matrix must use the same Junos OS version. For information about hardware and software requirements, see the *TX Matrix Plus Router Hardware Guide*.

TX Matrix Plus Router Software Upgrades and Reinstallation

By default, when you upgrade or reinstall software on the TX Matrix Plus router, the new software image is distributed to the connected T1600 routers. Software installed on a primary TX Matrix Plus router is distributed to all connected primary T1600 routers and the backup is distributed to all connected backup routers.

TX Matrix Plus Router Rebooting Process

When you reboot the TX Matrix Plus router master Routing Engine, all the master Routing Engines in the connected T1600 routers reboot. In addition, you can selectively reboot the master Routing Engine or any of the connected T1600 routers.

TX Matrix Plus Router Routing Engine Rebooting Sequence

The Routing Engines on the TX Matrix Plus router (or switch-fabric chassis) and T1600 routers (or line-card chassis) in the routing matrix boot from the storage media in this order: the USB device (if present), the CompactFlash card (if present), the disk (if present) in slot 1, and then the LAN.

TX Matrix Plus Router Management Ethernet Interfaces

The management Ethernet interface used for the TX Matrix Plus router and the T1600 routers in a routing matrix is **em0**. This interface provides an out-of-band method for connecting to the routers in the routing matrix. The Junos OS automatically creates the router's management Ethernet interface, em0. To use **em0** as a management port, you must configure its logical port, **em0.0**, with a valid IP address.

NOTE:

- The Routing Engines in the TX Matrix Plus router and in the T1600 routers configured in a routing matrix do not support the management Ethernet interface **fxp0** or the internal Ethernet interfaces **fxp1** or **fxp2**.
- Automated scripts that have been developed for standalone T1600 routers (T1600 routers not configured in a routing matrix) might contain references to the **fxp0**, **fxp1**, or **fxp2** interfaces. Before reusing the scripts on T1600 routers in a routing matrix, edit any command lines that reference the T1600 router management Ethernet interface **fxp0** by replacing "fxp0" with "em0".

TX Matrix Plus Router Internal Ethernet Interfaces

On a TX Matrix Plus router, the Routing Engine (RE-TXP-SFC) and Control Board (TXP-CB) function as a unit, or host subsystem. For each host subsystem in the router, the Junos OS automatically creates two internal Ethernet interfaces, **ixgbe0** and **ixgbe1**, for the two 10-Gigabit Ethernet ports on the Routing Engine.

Routing Matrix-Based T1600 Router Internal Ethernet Interfaces

On a T1600 router configured in a routing matrix, the Routing Engine (RE-TXP-LCC) and Control Board (LCC-CB) function as a unit, or host subsystem. For each host subsystem in the router, the Junos OS automatically creates two internal Ethernet interfaces, **bcm0** and **em1**, for the two Gigabit Ethernet ports on the Routing Engine.

For more information about the management Ethernet interface and internal Ethernet interfaces on a TX Matrix Plus router and T1600 routers configured in a routing matrix, see the *Junos OS Network Interfaces Configuration Guide*.

Committing Configurations on the TX Matrix Plus Router

In a routing matrix composed of a TX Matrix Plus router and T1600 routers, all configuration must be performed on the TX Matrix Plus router. Any configuration you commit on a T1600 router is not propagated to the TX Matrix Plus router or other T1600 routers. Only configuration changes you commit on the TX Matrix Plus router are propagated to all T1600 routers. A commit on a TX Matrix Plus router overrides any changes you commit on a T1600 router.

If you issue the **commit** command, you commit the configuration to all the master Routing Engines in the routing matrix.

```
user@host# commit
sfc-re0:
configuration check succeeds
lcc0-re0:
commit complete
lcc1-re0:
commit complete
sfc-re0:
commit complete
```

NOTE: **If a commit operation fails on any node, then the commit operation is not completed for the entire TX Matrix Plus router.**

If you issue the **commit synchronize** command on the TX Matrix Plus router, you commit the configuration to all the master and backup Routing Engines in the routing matrix.

```
user@host# commit synchronize
sfc-re0:
configuration check succeeds
lcc0-re1:
commit complete
lcc0-re0:
commit complete
lcc1-re1:
commit complete
lcc1-re0:
commit complete
sfc-re1:
commit complete
```



```
sfc-re0:
commit complete
```

Routing Matrix 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 Plus router. In addition, the routing matrix supports group names for the Routing Engines for each T1600 router: **lcc** ***n*****-re0** and **lcc** ***n*****-re1**. ***n*** identifies a T1600 router from 0 through 3.

Routing Matrix System Log Messages

You configure the T1600 routers to forward their system log messages to the TX Matrix Plus router at the **[edit system syslog host sfc0-master]** hierarchy level. For information about how to configure system log messages on a routing matrix based on the TX Matrix Plus router or the T1600 routers, see "Configuring System Logging for a TX Matrix Plus Router" on page 176.

Related Documentation

- Using the Junos OS to Configure a T1600 Router Within a Routing Matrix on page 819
- TX Matrix Plus Router Chassis and Interface Names on page 820
- Configuring the Junos OS to Upgrade the T1600 Router Chassis to LCC0 of a TX Matrix Plus Routing Platform on page 822

Using the Junos OS to Configure a T1600 Router Within a Routing Matrix

A routing matrix composed of a TX Matrix Plus router and T1600 routers supports the same chassis configuration statements as a standalone router (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 T1600 routers. In addition, a TX Matrix Plus router has two more chassis configuration statements, **online-expected** and **offline**.

To configure a T1600 router that is connected to a TX Matrix Plus router, include the **lcc** statement at the **[edit chassis]** hierarchy level:

```
[edit chassis]
lcc number;
```

number can be 0 through 3.

To configure a T1600 router 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;
  q-pic-large-buffer {
    large-scale;
  }
```

NOTE: For the FPC slot number, specify the actual hardware slot number (numbered 0 through 7) as labeled on the T1600 router chassis. Do not use the corresponding software FPC number shown in the "TX Matrix Plus Router Chassis and Interface Names" on page 820.

For information about how to configure the **online-expected** and **offline** configuration statements, see "Configuring the Junos OS to Enable the TX Matrix Plus Router to Generate an Alarm If a T1600 Router Stays Offline" on page 822.

Related Documentation

- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- TX Matrix Plus Router Chassis and Interface Names on page 820
- Configuring the Junos OS to Upgrade the T1600 Router Chassis to LCC0 of a TX Matrix Plus Routing Platform on page 822

TX Matrix Plus Router Chassis and Interface Names

The output from some CLI commands uses the terms SFC and **sfc** (for *switch-fabric chassis*) to refer to the TX Matrix Plus router. Similarly the terms LCC, and **lcc** as a prefix (for *line-card chassis*) refer to a T1600 router in a routing matrix composed of a TX Matrix Plus router and T1600 routers.

T1600 routers are assigned LCC index numbers, 0 through 3, depending on the hardware setup of the routing matrix. The current supported configuration of the routing matrix, can have up to four T1600 routers, and each T1600 router 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 OS CLI, an interface name has the following format:

type-*fpc/pic/port*

When you specify the FPC number, the Junos OS determines which T1600 router 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 T1600 routers to the correct FPC in a routing matrix, use the conversion chart shown in Table 52 on page 821. You can use the converted FPC number to configure the interfaces on the TX Matrix Plus router in your routing matrix.

Table 52: T1600 Router to Routing Matrix FPC Conversion Chart

FPC Numbering	T1600 Routers							
	LCC 0							
T1600 Router 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							
T1600 Router FPC Slots	0	1	2	3	4	5	6	7
Routing Matrix FPC Slots Equivalent	8	9	10	11	12	13	14	15
	LCC 2							
T1600 Router 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							
T1600 Router FPC Slots	0	1	2	3	4	5	6	7
Routing Matrix FPC Slots Equivalent	24	25	26	27	28	29	30	31

For example, in a routing matrix that contains **lcc 0** through **lcc 2**, **so-20/0/1** refers to FPC slot **4** of **lcc 2**.

Related Documentation

- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- Using the Junos OS to Configure a T1600 Router Within a Routing Matrix on page 819
- Configuring the Junos OS to Enable the TX Matrix Plus Router to Generate an Alarm If a T1600 Router Stays Offline on page 822

Configuring the Junos OS to Enable the TX Matrix Plus Router to Generate an Alarm If a T1600 Router Stays Offline

By default, the Junos OS enables all the T1600 routers in the routing matrix to come online. The Junos OS also enables you to configure all the T1600 routers so that if they do not come online, an alarm is sent by the TX Matrix Plus router.

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 T1600 router to be part of the routing matrix, you can configure it to be offline. This is useful when you are performing maintenance on a T1600 router. When the T1600 router is ready to come back online, delete the **offline** configuration statement.

To configure a T1600 router 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 T1600 router that is part of the routing matrix is allowed to come online. However, if a T1600 router does not come online, the TX Matrix Plus router does not generate an alarm.

Related Documentation

- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- Using the Junos OS to Configure a T1600 Router Within a Routing Matrix on page 819
- Configuring the Junos OS to Upgrade the T1600 Router Chassis to LCC0 of a TX Matrix Plus Routing Platform on page 822

Configuring the Junos OS to Upgrade the T1600 Router Chassis to LCC0 of a TX Matrix Plus Routing Platform

This topic provides an overview of the T1600 router configuration in order to upgrade it to the LCC0 of a newly configured TX Matrix Plus routing platform. The TX Matrix Plus routing platform consists of one TX Matrix Plus router that acts as the switch-fabric chassis (SFC) and from one to four T1600 routers that act as the line-card chassis (LCC). To perform the in-service upgrade, manually upgrade the Switch Interface Boards (SIBs), Control Boards (CBs) and Routing Engines of the T1600 router, and connect the upgraded T1600 router to the corresponding components of the TX Matrix Plus router with fiber-optic cables. When the SIBs of the T1600 router are upgraded and the data plane connection between the SFC and LCC is set up, the traffic flows in and out of the TX Matrix Plus routing platform through the data plane. When you upgrade the Routing Engines and CBs, the control plane connectivity between the SFC and LCC is set up. For information about the hardware and the installation requirements, see the *TX Matrix Plus Router Hardware Guide*.

This section discusses the following procedures to upgrade a standalone T1600 router to the LCC0 of a TX Matrix Plus routing platform:

Preparing the Configuration File and Upgrading the Junos OS on the T1600 Router and SFC

To prepare the configuration file and upgrade the Junos OS, follow these steps:

1. Save and archive a copy of the active configuration of the T1600 router.
2. Update the active configuration to make it applicable to the LCC.
3. Transfer the file configuration to the SFC (to be applied later).
4. Upgrade the T1600 router and SFC with Junos OS Release 10.1 or later, and reboot.

Configuring the Junos OS for Upgrading SIBs on the T1600 Router and Connecting It to the SFC

Upgrade the Control Boards (CBs) and Routing Engines of the T1600 router by replacing the T-CBs with LCC-CBs and RE 2000 with LCC-RE. To configure the T1600 router to support a SIB upgrade and connect it to the SFC, follow these steps:

1. Issue the **fabric upgrade-mode** CLI command at the **[edit chassis]** hierarchy level and commit the changes to update the configuration. This change in the configuration enables the T1600 chassis to be upgraded with the TXP-T1600 SIBs.

   ```
   [edit]
   user@host# set chassis fabric upgrade-mode
   user@host# commit
   ```

   You must also modify the configuration of the SFC by including **fabric upgrade-mode** statement at the **[edit chassis]** hierarchy level and commit the configuration on the SFC.

2. Take the backup SIB-I-T1600 offline by issuing the **request chassis sib slot *slot-number* offline** command.

   ```
   user@host> request chassis sib slot 0 offline
   ```

3. Replace the offline SIB-I-T1600 with SIB-TXP-T1600.

4. Bring the replaced SIB-TXP-T1600 online, by issuing the **request chassis sib slot *slot-number* online** command.

   user@host> **request chassis sib slot 0 online**

   The T1600 router automatically updates the links between the replaced SIB-TXP-T1600 and the Flexible PIC Concentrators (FPCs).

5. Establish the data plane connectivity by connecting the SIB-TXP-T1600 on the T1600 router to the ABS-SIB-F13 on the SFC with fiber-optic cables and configuring both routers (T1600 and SFC) for transmitting and receiving traffic on the TX Matrix Plus routing platform. Use the following CLI commands, to manually update the link between the T1600 router and SFC before the data plane is activated:

   - To configure the SFC to receive traffic from the T1600 router, issue the **request chassis sib f13 train-link-receive slot *SFC-SIB-F13-slot-num*** command.

     SFC-SIB-F13-slot-num is the slot in the SFC chassis where the ABS-SIB-F13 must be manually connected to SIB-TXP-T1600 in a slot (from 0 through 4) on the T1600 router. You can configure this for a value of 0, 3, 6, 8, or 11.

   - To configure the T1600 router to receive traffic from the SFC, issue the **request chassis sib train-link-receive slot *LCC-SIB-ST-SIB-L-slot-num*** command.

     LCC-SIB-ST-SIB-L-slot-num is the slot in the T1600 router chassis where SIB-TXP-T1600 must be manually connected to ABS-SIB-F13 in a slot (0, 3, 6, 8 or 11) on the SFC. You can configure this to be a value in the range from 0 through 4.

   - To configure the SFC to transmit traffic to the T1600 router, issue the **request chassis sib f13 train-link-transmit slot *SFC-SIB-F13-slot-num*** command.

     SFC-SIB-F13-slot-num is the slot in the SFC chassis where the ABS-SIB-F13 must be manually connected to SIB-TXP-T1600 in a slot (from 0 through 4) on the T1600 router. You can configure this for a value of 0, 3, 6, 8, or 11.

   - To configure the T1600 router to transmit traffic to the SFC, issue the **request chassis sib train-link-transmit slot *LCC-SIB-ST-SIB-L-slot-num*** command.

     LCC-SIB-ST-SIB-L-slot-num is the slot in the T1600 router chassis where SIB-TXP-T1600 must be manually connected to ABS-SIB-F13 in a slot (0, 3, 6, 8 or 11) on the SFC. You can configure this to be a value in the range from 0 through 4.

6. Using the SIB LEDs, manually verify the link between the T1600 router and the SFC. The FPCs will send traffic using the SIB-TXP-T1600 and ABS-SIB-F13.

7. Repeat Steps 2 through 4 for all the SIB-I-T1600s.

8. When all the SIBs are upgraded, delete the fabric upgrade-mode statement from the configuration hierarchy, and commit the changes on both the T1600 router and the SFC.

   [edit chassis]
   user@host# **delete chassis fabric upgrade-mode**
   user@host# **commit**

WARNING: You must upgrade the CBs and the Routing Engines of the T1600 router before you upgrade the SIBs.

Upgrading CBs and Routing Engines of the T1600 Router for Control Plane Connectivity

The CBs and the Routing Engines of the T1600 router are upgraded by replacing the T-CBs with LCC-CBs and RE-2000 with LCC-RE. To establish the control plane connectivity, connect the Ethernet cables from the T1600 router to the SFC. For more information about hardware requirements, see the *TX Matrix Plus Router Hardware Guide.*

Changing the Management Ethernet Interface Name for the T1600 Router

The Junos OS automatically configures management Ethernet interfaces for both the master and the backup Routing Engines, **fxp0**. However, after you upgrade both Routing Engines (master and backup), you must change the management Ethernet interface name to **em0**.

To change the management Ethernet interface name for the master Routing Engine, include the **interfaces em0** statement at the **[edit groups re0]** hierarchy level.

```
[edit groups re0]
user@host# set interfaces em0
user@host# commit
```

WARNING: If you do not change the management Ethernet interface from fxp0 to em0 for each upgraded LCC-RE, you cannot access the router remotely through services such as Telnet, SSH, and so on.

Transferring Control of the T1600 Router (LCC0) to the SFC

To transfer control from a T1600 router to the SFC, follow these steps:

1. Manually set the M/S switch on both replaced CBs of the T1600 router to M (multichassis).
2. Configure the T1600 router as LCC0 by including the **lcc *number*** statement at the **[edit chassis]** hierarchy level:

   ```
   [edit chassis]
   user@host>set lcc number
   ```

   NOTE: When you upgrade the other T1600 routers to LCC, you must set the LCC number from 1 to 3.

3. After you configure the LCC0, reboot it for the changes to take effect. This rebooting process establishes the forwarding state of the new LCC in the TX Matrix Plus routing platform by bringing up the SIBs automatically. For more information on hardware connectivity for the control plane, see the *TX Matrix Plus Router Hardware Guide*.

Adding a New T1600 Router to the TX Matrix Plus Routing Platform

The in-service upgrade of new operational T1600 routers to LCC1, LCC2, and LCC3 using the Junos OS CLI is not supported. To add a second LCC to the TX Matrix Plus routing platform, follow these steps:

1. Upgrade both the CBs and Routing Engines on the T1600 router. For details, see “Upgrading CBs and Routing Engines of the T1600 Router for Control Plane Connectivity” on page 825.
2. Upgrade the T1600 router with the same version of the Junos OS as on the SFC.
3. Upgrade the SIBs of the T1600 router and connect the new SIBs to the SFC. For details, see “Configuring the Junos OS for Upgrading SIBs on the T1600 Router and Connecting It to the SFC” on page 823.
4. Connect Ethernet links of the control plane from the T1600 router to the SFC.
5. Reboot the T1600 router. After rebooting, the router becomes a part of the TX Matrix Plus routing platform and is connected to the SFC on the control plane.

Downgrading a T1600 Router from the LCC of a TX Matrix Routing Platform to a Standalone T1600 Router

To downgrade any LCC to a standalone T1600 router, follow these steps:

1. Transfer the control to the LCC from the SFC:

   a. Roll back the configuration of the SFC and LCC to the configuration before the T1600 router was added and commit the configuration. For more information about configuring the T1600 router to LCC, see “Preparing the Configuration File and Upgrading the Junos OS on the T1600 Router and SFC” on page 823.

   b. Manually set the M/S switch to single-chassis on the T1600 router on both CBs.

   c. Reboot both the master and backup Routing Engines on the T1600.

2. Downgrade the SIBs of the LCC and remove the data plane connections:

   a. Take the spare SIB-TXP-T1600 on the LCC offline by issuing the **request chassis sib slot *slot-number* offline** command.

      user@host> **request chassis sib slot 0 offline**

   b. Remove the data plane connections from the SIB-TXP-T1600 to the SFC.

   c. Replace the SIB-TXP-T1600 with SIB-I-T1600 and bring it online.

   d. Repeat these steps for all SIB-TXP-T1600s.

3. Remove the control plane connectivity by disconnecting the Ethernet cables of the control plane from the T1600 router to the SFC.

The LCC becomes a standalone T1600 router out of the TX Matrix Plus routing platform.

Associating Sampling Instances for Active Flow Monitoring with a Specific Packet Forwarding Engine

The Junos OS enables you to configure sampling instances for active flow monitoring, by specifying a name for the sampling parameters and associating the instance name with a specific Packet Forwarding Engine.

To configure active sampling instances, include the **instance** statement at the **[edit forwarding-options sampling]** hierarchy level. This configuration is supported on MX Series, M120, M320, and T Series routers. For more information about configuring sampling instances, see the *Junos OS Services Interfaces Configuration Guide*.

To associate a configured active sampling instance with a specific Packet Forwarding Engine, include the sampling instance name at the **[edit chassis fpc *slot-number*]** hierarchy level:

```
[edit chassis fpc slot-number]
sampling-instance instance-name;
```

On a TX Matrix or TX Matrix Plus router, include the **sampling-instance** statement at the **[edit chassis lcc *number* fpc *slot-number*]** hierarchy level:

```
[edit chassis lcc number fpc slot-number]
sampling-instance instance-name;
```

Related Documentation

- *Junos Services Interfaces Configuration Guide*
- **sampling-instance on page 870**

CHAPTER 20

Summary of Router Chassis Configuration Statements

The following topics 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 OS Release 7.4.

Description Enable a service package on adaptive services interfaces.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable Service Packages on Adaptive Services Interfaces on page 770
- Configuring the Junos OS to Support Layer 2 Services on MX Series 3D Universal Edge Routers with MS-DPCs on page 770
- *Junos Services Interfaces Configuration Guide*
- *Junos OS Feature Guides*

aggregate-ports

Syntax aggregate-ports;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Release Information Statement introduced in Junos OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Specifying OC768-over-OC192 Mode

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 OS Release 7.4.
Support for LACP link protection and system priority introduced in Junos OS Release 9.3.

Description Configure properties for aggregated devices on the router.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS for Supporting Aggregated Devices on page 719

alarm

Syntax

```
alarm {
  interface-type {
    alarm-name (red | yellow | ignore);
  }
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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 either the router's craft interface or the switch's LCD screen and trigger an audible alarm if one is connected to the contact on the craft interface or LCD screen. Yellow alarm conditions light the **YELLOW ALARM** LED on either the router's craft interface or the switch's LCD screen and trigger an audible alarm if one is connected to the craft interface or LCD screen.

To configure more than one alarm, include multiple ***alarm-name*** lines.

Options *alarm-name*—Alarm condition. For a list of conditions, see Table 37 on page 736.

ignore—The specified alarm condition does not set off any alarm.

interface-type—Type of interface on which you are configuring the alarm: **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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Understanding Alarms
- Chassis Conditions That Trigger Alarms on page 737
- Chassis Alarm Messages on a QFX3500 Switch
- Interface Alarm Messages

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*] (Routing Matrix)

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an Asynchronous Transfer Mode (ATM) Physical Interface Card (PIC) in cell-relay accumulation mode.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Use ATM Cell-Relay Accumulation Mode on an ATM1 PIC on page 721

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*] (Routing Matrix)

Release Information Statement introduced before Junos OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable ATM2 Intelligent Queuing Layer 2 Circuit Transport Mode on page 788

bandwidth

Syntax bandwidth (1g | 10g);

Hierarchy Level [edit chassis fpc *slot-number* pic *number* tunnel-services]

Release Information Statement introduced in Junos OS Release 8.2.

Description On the MX Series 3D Universal Edge 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 a 10-Gigabit Ethernet 4-port DPC or a 16x10GE 3D MPC.

NOTE: **If you specify a bandwidth that is not compatible with the type of DPC or MPC and their respective 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 or 16x10GE 3D MPC.**

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters on page 790

ce1

Syntax

```
ce1 {
  e1 port-number {
    channel-group channel-number timeslots slot-number;
  }
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure channelized E1 port and channel specifications.

Options **e1** ***port-number***—Any valid E1 port number on the host system.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Channel Groups and Time Slots for Channelized E1 PICs on page 785

channel-group

Syntax channel-group *channel-number* timeslots *slot-number*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* ce1 e1 *link-number*],
[edit chassis fpc *slot-number* pic *pic-number* ct3 port *port-number* t1 *link-number*],
[edit chassis lcc *lcc-index* fpc *slot-number* pic *pic-number* ce1 e1 *link-number*],
[edit chassis lcc *lcc-index* fpc *slot-number* pic *pic-number* ct3 port *port-number* t1 *link-number*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the DS0 channel number.

Options ***channel-number***—DS0 channel group.

Range: 0 through 7 for DS0 naming, and 0 through 23 for E1 naming.

timeslots *slot-number*—One or more actual time slot numbers 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

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots on page 781
- Configuring the Junos OS to Support Channel Groups and Time Slots for Channelized E1 PICs on page 785

chassis

Syntax chassis { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure router chassis properties.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Router Chassis Configuration Statements on page 713

config-button

Syntax

```
config-button {
  no-clear;
  no-rescue;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Prevent the Resetting of the Factory Default or Rescue Configuration During Current Configuration Failure on J Series Routers on page 800

craft-lockout

Syntax craft-lockout;

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 8.1.

Description Disable the physical operation of the craft interface front panel.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable the Physical Operation of the Craft Interface on page 769

ct3

Syntax

```
ct3 {
  port port-number {
    t1 link-number {
      channel-group channel-number timeslots slot-number;
    }
  }
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots on page 781

device-count

Syntax device-count *number*;

Hierarchy Level [edit chassis **aggregated-devices ethernet**]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the number of aggregated logical devices available to the router.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for Supporting Aggregated Devices on page 719

disk-failure-action

Syntax disk-failure-action (halt | reboot);

Hierarchy Level [edit chassis routing-engine on-disk-failure]

Release Information Statement introduced in Junos OS Release 9.0.

Description 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable a Routing Engine to Reboot on Hard Disk Errors on page 799

e1

Syntax

e1 *port-number* {
  channel-group *channel-number* timeslots *slot-number*;
}

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* ce1]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the channelized E1 port number on the PIC. The range is from **0** through **9**.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Channel Groups and Time Slots for Channelized E1 PICs on page 785

egress-policer-overhead

Syntax egress-policer-overhead *bytes*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Release Information Statement introduced before Junos OS Release 11.1.

Description Add the configured number of bytes to the length of a packet exiting the interface.

Options *bytes*—Number of bytes added to a packet exiting an interface.

Range: 0–255 bytes

Default: 0

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring a Policer Overhead on page 784
- **ingress-policer-overhead on page 851**
- CoS on Enhanced IQ2 PICs Overview

ethernet (Chassis)

Syntax

```
ethernet {
  device-count number;
  lacp {
    link-protection {
      non-revertive;
    }
    system-priority;
  }
}
```

Hierarchy Level [edit chassis **aggregated-devices**]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure properties for Ethernet aggregated devices on the router.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for Supporting Aggregated Devices on page 719

family

Syntax

```
family {
  inet {
    layer-3;
    layer-4;
    symmetric-hash {
      complement;
    }
  }
  multiservice {
    source-mac;
    destination-mac;
    payload {
      ip {
        layer-3;
        layer-4;
      }
    }
    symmetric-hash {
      complement;
    }
  }
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* hash-key]

Release Information Statement introduced in Junos OS Release 9.6.

Description (MX Series 3D Universal Edge Routers only) Configure data used in a hash key for a specific protocol family when configuring PIC-level symmetrical load balancing on an 802.3ad Link Aggregation Group.

Options inet—Configure data used in a hash key for the **inet** protocol family.

multiservice—Configure data used in a hash key for the **multiservice** protocol family.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers on page 725

fabric upgrade-mode

Syntax

```
fabric {
  upgrade-mode;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 7.5.

Description Configure upgrade mode for SIBs and forces them to operate in the same mode until the upgrade is complete.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808

filter

Syntax filter;

Hierarchy Level [edit chassis **memory-enhanced**]

Release Information Statement added in Junos OS Release 11.1.

Description Enables storing of firewall filters across multiple static RAM (SRAM) segments, resulting in proper utilization of SRAM segments. This feature is useful in routers with small routing tables and large firewall filters. This statement is supported on T Series routers.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Allocate More Memory for Routing Tables, Firewall Filters, and Layer 3 VPN Labels on page 792

fpc (M320, T320, T640 Routers)

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 OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs on page 772
- Configuring the Junos OS to Enable a SONET PIC to Operate in Channelized (Multiplexed) Mode on page 780

fpc (MX Series 3D Universal Edge Routers)

Syntax

```
fpc slot-number {
  pic number {
    port-mirror-instance port-mirroring-instance-name-pic-level;
    tunnel-services {
      bandwidth (1g | 10g)
    }
  }
  port-mirror-instance port-mirroring-instance-name-fpc-level;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 8.2.
port-mirror-instance option introduced in Junos OS Release 9.3.

Description On MX Series 3D Universal Edge Routers only, configure properties for the DPC or MPC and corresponding Packet Forwarding Engines to create tunnel interfaces.

Configure a port-mirroring instance for the DPC and its corresponding Packet Forwarding Engines.

(MX Series Virtual Chassis only) To configure properties for DPCs or MPCs in a member router in an MX Series Virtual Chassis configuration, you must specify the router's Virtual Chassis member number *before* the **fpc** statement. Specify the member number in the form **member *member-id***, where ***member-id*** is 0 or 1. If you do not specify the member number before the **fpc** statement, the commit operation fails and the software displays an error message indicating that the **fpc** statement must include the member number for routers in Virtual Chassis mode.

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 *port-mirroring-instance-name-fpc-level*—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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters on page 790
- Configuring Port-Mirroring Instances on MX Series 3D Universal Edge Routers on page 722

fpc (TX Matrix and TX Matrix Plus Routers)

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 OS Release 7.4.

Description On a TX Matrix or TX Matrix Plus router, 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808
- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs on page 772
- TX Matrix Router Chassis and Interface Names on page 811
- TX Matrix Plus Router Chassis and Interface Names on page 820

fpc-feb-connectivity

Syntax
```
fpc-feb-connectivity {
  fpc number feb (slot-number | none);
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS 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—Disconnect the FPC from the FEB.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS to Support FPC to FEB Connectivity on M120 Routers on page 798

fpc-resync

Syntax fpc-resync;

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 10.2.

Description (On M320, T320, T640, T1600, TX Matrix, and TX Matrix Plus routers only) When a Flexible PIC Concentrator (FPC) is brought online, resynchronize the sequence numbers of the FPC with the other active FPCs.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS to Resynchronize FPC Sequence Numbers with Active FPCs when an FPC Comes Online on page 718
- *TX Matrix Router Hardware Guide*

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 OS Release 7.4.

Description On SONET/SDH PICs only, configure the framing type.

Default **sonet**

Options **sdh**—SDH framing.

sonet—SONET framing.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs on page 772

fru-poweron-sequence

Syntax fru-poweron-sequence;

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 10.0.

Description (MX Series 3D Universal Edge Routers only) Configure the power-on sequence for the DPCs in the chassis for routers with the enhanced AC Power Entry Module (PEM).

Options None.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring the Power-On Sequence for DPCs on MX Series Routers with the Enhanced AC PEM on page 734

hash-key

Syntax

```
hash-key {
  family {
    inet {
      layer-3;
      layer-4;
      symmetric-hash {
        complement;
      }
    }
    multiservice {
      source-mac;
      destination-mac;
      payload {
        ip {
          layer-3 (source-ip-only | destination-ip-only);
          layer-4;
        }
      }
    }
  }
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Release Information Statement introduced in Junos OS Release 9.6.

Description (MX Series 3D Universal Edge Routers only) Configure data used in a hash key for a PIC for symmetrical load balancing on an 802.3ad Link Aggregation Group.

Options **family**—Configure data used in a hash key for a protocol family. This statement has the following suboptions:

- **inet**—Configure data used in a hash key for the **inet** protocol family.
- **multiservice**—Configure data used in a hash key for the **multiservice** protocol family.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers on page 725

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] (Routing Matrix)

Release Information Statement introduced before Junos OS 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)

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable Idle Cell Format and Payload Patterns for ATM Devices on page 795

inet

Syntax

```
inet {
  layer-3;
  layer-4;
  symmetric-hash {
    complement;
  }
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* hash-key family]

Release Information Statement introduced in Junos OS Release 9.6.

Description (MX Series 3D Universal Edge Routers only) Configure data used in a hash key for the **inet** protocol family when configuring PIC-level symmetrical load balancing on an 802.3ad Link Aggregation Group.

Options layer-3—Include Layer 3 IP data in the hash key.

layer-4—Include Layer 4 IP data in the hash key.

symmetric-hash—Configure symmetric hash key with source and destination ports.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers on page 725

ingress-policer-overhead

Syntax ingress-policer-overhead *bytes*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Release Information Statement introduced before Junos OS Release 11.1

Description Add the configured number of bytes to the length of a packet entering the interface.

Options *bytes*—Number of bytes added to a packet entering an interface.

Range: 0–255 bytes

Default: 0

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring a Policer Overhead on page 784
- **egress-policer-overhead on page 840**
- CoS on Enhanced IQ2 PICs Overview

lacp

Syntax

```
lacp {
  link-protection {
    non-revertive;
  }
  system-priority priority;
}
```

Hierarchy Level [edit chassis aggregated-devices ethernet]

Release Information Statement introduced in Junos OS 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.

Options The statements are described separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for Supporting Aggregated Devices on page 719

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;
  }
  q-pic-large-buffer {
    large-scale;
  }
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a T640 router (on a routing matrix based on a TX Matrix router) or a T1600 router (on a routing matrix based on a TX Matrix Plus router).

Options *number*—Specify a T640 router or a T1600 on a routing matrix.

Range: 0 through 3

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808
- Using the Junos OS to Configure a T640 Router Within a Routing Matrix on page 810
- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- Using the Junos OS to Configure a T1600 Router Within a Routing Matrix on page 819
- *TX Matrix Router Hardware Guide*
- *TX Matrix Plus Router Hardware Guide*

linerate-mode

Syntax linerate-mode;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* linerate-mode],
[edit chassis lcc *number* fpc *slot-number* pic *pic-number* linerate-mode] (Routing Matrix)

Release Information Statement introduced in Junos OS Release 10.1.

Description For 10-port 10-Gigabit Oversubscribed Ethernet (OSE) PICs only, configure the line rate operation.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Network Interfaces Configuration Guide*

link-protection

Syntax
```
link-protection {
  non-revertive;
}
```

Hierarchy Level [edit chassis aggregated-devices ethernet lacp]

Release Information Statement introduced in Junos OS Release 9.3.

Description Enable LACP link protection at the global (chassis) level.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS for Supporting Aggregated Devices on page 719

maximum-ecmp

Syntax maximum-ecmp *next-hops*;

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 10.1.

Description (M10i routers with Enhanced CFEB, and M320, M120, MX Series, and T Series routers) Configure 16, 32, or 64 ECMP next hops for RSVP or LDP LSPs.

Default 16

Options ***next-hops***—Specify the number of next hops (16, 32, or 64) for the RSVP or LDP LSPs.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring ECMP Next Hops for RSVP and LDP LSPs for Load Balancing on page 729

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*] (Routing Matrix)

Release Information Statement introduced before Junos OS Release 7.4.

Description On M320, T320, T640 , TX Matrix, and TX Matrix Plus routers, configure eight egress queues on IQ interfaces.

On MX Series routers, configure eight egress queues on Trio MPC/MIC interfaces.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Eight Queues on IQ Interfaces for T Series and M320 Routers on page 783
- Configuring the Maximum Number of Queues for Trio MPC/MIC Interfaces

memory-enhanced

Syntax

```
memory-enhanced {
  filter;
  route;
  vpn-label;
}
```

Hierarchy Level [edit chassis]

Release Information Statement added in Junos OS Release 10.4.

Description Allocate more jtree memory for routing tables and Layer 3 VPNs.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Allocate More Memory for Routing Tables, Firewall Filters, and Layer 3 VPN Labels on page 792

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 OS 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

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support the Link Services PIC on page 794
- *Junos Network Interfaces Configuration Guide*

multiservice

Syntax

```
multiservice {
  source-mac;
  destination-mac;
  payload {
    ip {
      layer-3 (source-ip-only | destination-ip-only);
      layer-4;
    }
  }
  symmetric-hash {
    complement;
  }
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* hash-key family]

Release Information Statement introduced in Junos OS Release 9.6.

Description (MX Series 3D Universal Edge Routers only) Configure data used in a hash key for the **multiservice** protocol family when configuring PIC-level symmetrical hashing for load balancing on an 802.3ad Link Aggregation Group.

Options destination-mac—Include destination MAC address in the hash key.

payload—Include payload data in the hash key. This option has the following suboptions:

- **layer-3**—Include Layer 3 IP information in the hash key.
- **layer-4**—Include Layer 4 IP information in the hash key.

source-mac—Include source MAC address in the hash key.

symmetric-hash—Create a symmetric hash or symmetric hash complement key with any attribute.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers on page 725

network-services

Syntax network-services (ethernet | ip);

Hierarchy Level [edit chassis]

Release Information Statement introduced before Junos OS Release 8.5.

Description Set the router's network services to either Ethernet or Internet Protocol (IP).

Options **ethernet**—Set the router's network services to Ethernet.

ip—Set the router's network services to Internet Protocol.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Run in the IP and Ethernet Services Mode in MX Series Routers on page 805

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 OS 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**.

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).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable a SONET PIC to Operate in Channelized (Multiplexed) Mode on page 780
- *Junos Network Interfaces Configuration Guide*

no-multi-rate

Syntax no-multi-rate;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Disable the rate-selectability configuration. This statement is supported only on the 8-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP. The **no-multi-rate** statement has no effect on the 4-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, which is always rate-selectable.

Default Rate-selectability is enabled.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring a Port Speed on page 773

non-revertive

Syntax non-revertive;

Hierarchy Level [edit chassis aggregated-devices ethernet lacp link-protection]

Release Information Statement introduced in Junos OS 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 interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for Supporting Aggregated Devices on page 719

number-of-ports

Syntax number-of-ports *active-ports*;

Hierarchy Level [edit chassis fpc *slot-number*]

Release Information Statement introduced in Junos OS Release 10.1.

Description Enable or disable 8 or 12 physical ports on a 16-port 10-Gigabit Ethernet MPC (16x10GE 3D MPC).

Options ***active-ports***—Specify the number of ports (8 or 12) to enable or disable.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Number of Active Ports on a 16-Port 10-Gigabit Ethernet MPC on MX Series Routers on page 732

offline

Syntax offline;

Hierarchy Level [edit chassis lcc *number*]

Release Information Statement introduced before Junos OS Release 7.4.

Description (Routing matrix based on the TX Matrix and TX Matrix Plus routers only) On a TX Matrix router, configure a T640 router so that it is not part of the routing matrix. On a TX Matrix Plus router, configure a T1600 router so that it is not part of the routing matrix.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **online-expected on page 860**
- TX Matrix Router and T640 Router Configuration Overview on page 808
- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- Configuring the Junos OS to Enable the TX Matrix Router to Generate an Alarm If a T640 Router Stays Offline on page 814
- Configuring the Junos OS to Enable the TX Matrix Plus Router to Generate an Alarm If a T1600 Router Stays Offline on page 822

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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable a Routing Engine to Reboot on Hard Disk Errors on page 799

online-expected

Syntax online-expected;

Hierarchy Level [edit chassis **lcc** *number*]

Release Information Statement introduced before Junos OS Release 7.4.

Description (TX Matrix and TX Matrix Plus routing matrix only) On a TX Matrix router, configure a T640 router so that if it does not come online, an alarm is sent to the TX Matrix router. On a TX Matrix Plus router, configure a T1600 router so that if it does not come online, an alarm is sent to the TX Matrix Plus router.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808
- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- Configuring the Junos OS to Enable the TX Matrix Router to Generate an Alarm If a T640 Router Stays Offline on page 814
- Configuring the Junos OS to Enable the TX Matrix Plus Router to Generate an Alarm If a T1600 Router Stays Offline on page 822
- **offline on page 859**

packet-scheduling

Syntax (packet-scheduling | no-packet-scheduling);

Hierarchy Level [edit chassis]

Release Information Statement introduced before Junos OS Release 7.4.

Description (M 160 routers only) 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable an M160 Router to Operate in Packet Scheduling Mode on page 791

payload

Syntax

```
payload {
  ip {
    layer-3;
    layer-4;
  }
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* hash-key family multiservice]

Release Information Statement introduced in Junos OS Release 9.6.

Description (MX Series 3D Universal Edge Routers only) Include payload data in a hash key for the **multiservice** protocol family when configuring PIC-level symmetrical load balancing on an 802.3ad Link Aggregation Group.

Options **ip**—Include IPv4 payload data in the hash key. This option has the following suboptions:

- **layer-3**—Include Layer 3 IP information in the hash key.
- **layer-4**—Include Layer 4 IP information in the hash key.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers on page 725

pem

Syntax

```
pem {
  minimum number;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 7.4.

Description Configure the minimum number of Power Entry Modules (PEMs) on an M320 router. With this configuration, PEM absent alarms are generated only if the PEM count falls below the minimum specified.

Options **minimum *number***—Minimum number of PEMs on the router.

Range: 0 through 3

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Entry-Level Configuration on an M320 Router with a Minimum Number of SIBs and PIMs on page 803
- **sib on page 871**

pic (M Series and T Series Routers)

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 OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs on page 772
- Configuring the Junos OS to Enable a SONET PIC to Operate in Channelized (Multiplexed) Mode on page 780
- Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots on page 781
- Configuring the Junos OS to Support Channel Groups and Time Slots for Channelized E1 PICs on page 785

pic (TX Matrix and TX Matrix Plus Routers)

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 OS Release 7.4.

Description On a TX Matrix or TX Matrix Plus router, 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- TX Matrix Router and T640 Router Configuration Overview on page 808
- TX Matrix Plus Router and T1600 Router Configuration Overview on page 815
- Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs on page 772

port

Syntax port *port-number*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* ct3]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the channelized T3 port number on the PIC.

Options ***port-number***—Port number.

Range: 0 through 1

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots on page 781

power

Syntax power (off | on);

Hierarchy Level [edit chassis fpc *slot-number*]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Make a Flexible PIC Concentrator Stay Offline on page 717

q-pic-large-buffer

Syntax q-pic-large-buffer (large-scale | small-scale);

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 OS Release 7.4.

Description Configure delay buffers.

NOTE: When you commit the configuration after including the **q-pic-large-buffer** statement for a PIC, the Junos OS temporarily takes the PIC offline and brings it back online before the new configuration is activated and becomes the current operational configuration.

Default **small-scale**

Options **large-scale**—(Optional) 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—(Optional) Set the average packet size used to calculate the number of notification queue entries in the IQ PIC to 40 bytes.

NOTE: You cannot configure the **large-scale** and the **small-scale** options on MX Series routers. Include only the **q-pic-large-buffer** statement to enable the large delay buffer size on Enhanced Queuing DPCs on MX Series routers.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable Larger Delay Buffers for T1, E1, and DS0 Interfaces Configured on Channelized IQ PICs on page 801
- *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 OS Release 8.3.

Description

Configure computation of buffer occupancy weighted RED (WRED) based on weighted-averaging of buffer occupancy on an IQ PIC.

Options

weighted-averaged—Configure weighted-averaging of buffer occupancy on an IQ PIC. This option has the following suboption:

instant-usage-weight-exponent ***weight-value***—(Optional) Establish an exponent and instant buffer usage weight value 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.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos Class of Service Configuration Guide*

route

Syntax

route;

Hierarchy Level

[edit chassis **memory-enhanced**]

Release Information

Statement added in Junos OS Release 10.4.

Description

Allocate more jtree memory for routing tables over firewall filters.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Allocate More Memory for Routing Tables, Firewall Filters, and Layer 3 VPN Labels on page 792

routing-engine

Syntax

```
routing-engine {
  on-disk-failure {
    disk-failure-action (halt | reboot);
  }
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced before Junos OS Release 7.4.
The **disk-failure-action** statement added in Junos OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable a Routing Engine to Reboot on Hard Disk Errors on page 799
- *Junos High Availability Configuration Guide*

sfm

Syntax sfm *slot-number* power off;

Hierarchy Level [edit chassis]

Release Information Statement introduced before Junos OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Make an SFM Stay Offline on page 717
- *Junos High Availability Configuration Guide*

sampling-instance

Syntax sampling-instance *instance-name*;

Hierarchy Level [edit chassis fpc *slot-number*]
[edit chassis lcc *number* fpc *slot-number*] (Routing Matrix)

Release Information Statement introduced in Junos OS Release 9.6.

Description (MX Series, M120, M320, and T Series routers only) Associate a defined sampling instance with a specific Packet Forwarding Engine for active sampling instances configured at the **[edit forwarding-options sampling]** hierarchy level.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Associating Sampling Instances for Active Flow Monitoring with a Specific Packet Forwarding Engine on page 827
- *Junos Services Interfaces 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 OS Release 7.4.
Statement introduced on MX Series 3D Universal Edge Routers with MS-DPCs in Junos OS Release 9.6.

Description For adaptive services interfaces, enable a service package on the specified Physical Interface Card (PIC).

Default **layer-3**

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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable Service Packages on Adaptive Services Interfaces on page 770
- Configuring the Junos OS to Support Layer 2 Services on MX Series 3D Universal Edge Routers with MS-DPCs on page 770
- *Junos Services Interfaces Configuration Guide*

session-offload

Syntax session-offload;

Hierarchy Level **[edit chassis fpc *slot-number* pic *number* adaptive-services service-package extension-provider]**

Release Information Statement introduced on MX Series 3D Universal Edge Routers with MS-DPCs in Junos OS Release 9.6.

Description Enable session offloading on a per-PIC basis for a Multiservices PIC.

Default Session offloading is disabled.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable Session Offloading on MX Series 3D Universal Edge Routers with MS-DPCs on page 771

sib

Syntax

```
sib {
  minimum number;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS 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

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Entry-Level Configuration on an M320 Router with a Minimum Number of SIBs and PIMs on page 803
- **pem on page 863**

sonet

Syntax

```
sonet {
  device-count number;
}
```

Hierarchy Level [edit chassis **aggregated-devices**]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure properties for SONET/SDH aggregated devices on the router.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS for Supporting Aggregated Devices on page 719

sparse-dlcis

Syntax sparse-dlcis;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*];

Release Information Statement introduced before Junos OS Release 7.4.

Description Support a full data-link connection identifier (DLCI) range (1 through 1022). This enables you to use circuit cross-connect (CCC) and translation cross-connect (TCC) features by means of Frame Relay on T1 and E1 interfaces.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support the Sparse DLCI Mode on Channelized STM1 or Channelized DS3 PICs on page 779

speed

Syntax speed (oc3-stm1 | oc12-stm4 | oc48-stm16);

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* port *port-number*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure the port speed. This statement is supported only on SONET/SDH (Multi-Rate) MICs with SFP.

Default **oc3-stm1**

Options **oc3-stm1**—OC3 or STM1.

oc12-stm4—OC12 or STM4.

oc48-stm16—OC48 or STM16.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring a Port Speed on page 773

symmetric-hash

Syntax

```
symmetric-hash {
  complement;
}
```

Hierarchy Level [edit chassis fpc slot-number pic slot-number hash-key family inet],
[edit chassis fpc slot-number pic slot-number hash-key family multiservice]

Release Information Statement introduced in Junos OS Release 9.6.

Description (MX Series 3D Universal Edge Routers only) Configure the symmetric hash or symmetric hash complement at the PIC level for configuring symmetrical load balancing on an 802.3ad Link Aggregation Group.

Options complement—Include the complement of the symmetric hash in the hash key.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers on page 725

synchronization (M Series, T Series)

Syntax

```
synchronization {
  primary (external-a | external-b);
  secondary (external-a | external-b);
  signal-type (t1 | e1);
  switching-mode (revertive | non-revertive);
  transmitter-enable;
  validation-interval seconds;
  y-cable-line-termination;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced on the M120 router in Junos OS Release 9.3.
Statement introduced on the T320, T640, and T1600 routers in Junos OS Release 10.2.

Description (M320, M40e, M120, T320, T640, and T1600 routers only) Configure an external synchronization interface to synchronize the internal Stratum 3 clock to an external source, and then synchronize the chassis interface clock to that source.

Options **primary**—First external timing source specified in the configuration hierarchy. This statement has the following suboptions:

- **external-a**—Use **external-a** as the primary clock synchronization source.
- **external-b**—Use **external-b** as the primary clock synchronization source.

secondary—Second external timing source specified in the configuration hierarchy.

- **external-a**—Use **external-a** as the secondary clock synchronization source.
- **external-b**—Use **external-b** as the secondary clock synchronization source.

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**

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, M40e, T320, T640, and T1600 routers) 90 through 86400 seconds. (M120 routers) 30 through 86400 seconds.

Default: (M320, M40e, T320, T640, and T1600 routers) 90 seconds. (M120 routers) 30 seconds

y-cable-line-termination—(M320 routers only) Specify that a single signal be wired to both Control Boards (CBs) using a Y-cable.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support an External Clock Synchronization Interface for M Series and T Series Routers on page 775

synchronization (MX Series)

Syntax

```
synchronization {
  clock-mode (auto-select | free-run);
  esmc-transmit {
    interfaces (all | interface-name);
  }
  hold-interval {
    configuration-change seconds;
    restart seconds;
    switchover seconds;
  }
  network-type (option-1 | option-2);
  quality-mode-enable;
  switchover-mode (revertive | non-revertive);
  source {
    (external-a | external-b) {
      priority number;
      quality-level (prc | prs |sec | smc | ssu-a | ssu-b | st2 | st3 | st3e | st4 | stu | tnc);
      request (force-switch | lockout);
    }
    interfaces interface-name {
      priority number;
      quality-level (prc | prs |sec | smc | ssu-a | ssu-b | st2 | st3 | st3e | st4 | stu | tnc);
      request (force-switch | lockout);
      wait-to-restore minutes;
    }
  }
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 10.4.

Description (MX80 and MX240 routers only) Configure the synchronous Ethernet (SyncE) parameters.

Options

clock-mode (auto-select | free-run)—Specify the mode of operation to select the clock source either from free-run local oscillator or from an external qualified clock. On MX80 routers, the free-run clock is provided by the SCB and on MX240 with MPC, it is provided by a local oscillator. The default setting is auto-select mode.

esmc-transmit interfaces (all | *interface-name*)—Enables Ethernet Synchronization Message Channel (ESMC) packet transmission.

hold-interval (configuration-change | restart | switchover) *seconds*—Specify the chassis synchronization hold-interval:

- Time interval to wait before selecting the new clock source during.
- The default switchover is 30 seconds. Cold reboot is 120 seconds.

network-type (option-1 | option-2)—Specify the clock type: EEC-1 maps to G.813 option 1 or EEC-2 maps to G.812 type IV clock.

quality-mode-enable—Specify the clock selection, quality level, and priority setting. The default setting is disable.

switchover-mode (revertive | non-revertive)—Specify revertive or non-revertive switchover mode:

- In revertive mode, the system switches from a lower to a higher quality clock source whenever the higher clock source becomes available.
- In non-revertive mode, the system continues to use the current clock source as long as it is valid.
- The default is revertive mode.

source (external-a | external-b | interfaces *interface-name*)—Specify a clock source. The clock source is specified using the clock selection process.

- **priority *number***—(Optional) A priority level between 1 and 5. When not specified, external-a has higher default priority than external-b, and external-b has higher default priority than other Gigabit Ethernet or 10-Gigabit Ethernet clock sources, which have the lowest default priority. Configured priority is higher than any default priority.
- **quality-level (prc | prs |sec | smc | ssu-a | ssu-b | st2 | st3 | st3e | st4 | stu | tnc)**—Specify the clock type. Specific **quality-level** options are valid depending on the configured **network-type**, **option-1** or **option-2**.
  - Both option I and option II SSM quality levels (QL) are supported:
    - For option-1, QL must be configured for external clocks (extern-a or extern-b) whether or not QL is enabled 3.
    - For option-2, the default QL for external clocks is QL_STU whether or not QL is enabled.
  - QL is set to DNU for network-option 1 and set to DUS for network-option 2, if quality-level not configured and no ESMC messages received.
  - On selected active source (primary or secondary which is active), even if ESMC transmit is not enabled, a DNU ESMC will be sent out if network-option is 1, and DUS ESMC will be sent out if network-option is 2. This is applicable only for sources of type ethernet interface. This is done to avoid the source looping as per the standard requirement.
- **request force-switch**—Forces a switch to the source provided the source is enabled and not locked out. Only one configured source may be force-switched.
- **request lockout**—Lockout may be configured for any source. When configured, that source will not be considered by the selection process.
- **wait-to-restore *minutes***—You can specify a time for each port. When a port's signal transitions out of the signal fail state, it must be fault free for the **wait-to-restore** time before it is again considered by the selection process.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring an External Clock Synchronization Interface for MX Series Routers on page 776
- request chassis synchronization mode

system-priority

Syntax system-priority *priority*;

Hierarchy Level [edit chassis aggregated-devices ethernet lacp]

Release Information Statement introduced in Junos OS 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 Documentation
- Configuring the Junos OS for Supporting Aggregated Devices on page 719

t1

Syntax

t1 *link-number* {
  channel-group *channel-number* timeslots *slot-number*;
}

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* ct3 port *port-number*];

Release Information Statement introduced before Junos OS 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Channelized DS3-to-DS0 Naming for Channel Groups and Time Slots on page 781

traffic-manager

Syntax

```
traffic-manager {
  egress-shaping-overhead number;
  ingress-shaping-overhead number;
  mode {
    egress-only;
    ingress-and-egress;
    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 OS Release 8.3.

Description

Enable CoS queueing, scheduling, and shaping.

NOTE: Junos OS does not support ingress-and-egress mode on label-switched interfaces (LSI) configured with VPLS .

Options

egress-shaping-overhead ***number***—When traffic management (queueing and scheduling) is configured on the egress side, the number of CoS shaping overhead bytes to add to the packets on the egress interface.

Replace ***number*** with a value from **-63** through **192** bytes.

ingress-shaping-overhead ***number***—When L2TP session shaping is configured, the number of CoS shaping overhead bytes to add to the packets on the ingress side of the L2TP tunnel to determine the shaped session packet length.

When session shaping is not configured and traffic management (queueing and scheduling) is configured on the ingress side, the number of CoS shaping overhead bytes to add to the packets on the ingress interface.

Replace ***number*** with a value from **—63** through **192** bytes.

mode—Configure CoS traffic manager mode of operation. This option has the following suboptions:

- **egress-only**—Enable CoS queuing and scheduling on the egress side for the PIC that houses the interface. This is the default mode for an Enhanced Queueing (EQ) DPC on MX Series routers.

  NOTE: If ingress packet drops are observed at a high rate for an IQ2 or IQ2E PIC, configure the **traffic-manager** statement to work in the **egress-only** mode.

- **ingress-and-egress**—Enable CoS queueing and scheduling on both the egress and ingress sides for the PIC. This is the default mode for IQ2 and IQ2E PICs on M Series and T Series routers.

NOTE:
- For EQ DPCs, you must configure the **traffic-manager** statement with **ingress-and-egress** mode to enable ingress CoS on the EQ DPC.
- EQ DPCs have 250 ms of buffering, with only egress queueing (default mode). When **ingress-and-egress** is configured, the buffer is partitioned as 50 ms for the ingress direction and 200 ms for the egress direction.

- **session-shaping**—(M10i and M120 routers only) Configure the IQ2 PIC mode for session-aware traffic shaping to enable L2TP session shaping.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos Class of Service Configuration Guide*

tunnel-services

Syntax

```
tunnel-services {
  bandwidth (1g | 10g);
  tunnel-only;
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *number*]

Release Information Statement introduced in Junos OS Release 8.2.

Description For MX Series 3D Universal Edge Routers, configure the amount of bandwidth for tunnel services.

For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, configure support for per unit scheduling for GRE tunnels. Use the **tunnel-services** statement to specify that the IQ2 or IQ2E PIC will work both as a regular PIC and as a tunnel PIC. For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, you can use the **tunnel-only** option to specify that an IQ2 or IQ2E PIC work in tunnel mode only.

Options **tunnel–only** (Optional)—For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, specify that an IQ2 or IQ2E PIC work in tunnel mode only.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Tunnel Interfaces on MX Series 3D Universal EdgeRouters on page 790

ucode-imem-remap

Syntax ucode-imem-remap;

Hierarchy Level [edit chassis feb slot *number*]

Release Information Statement introduced in Junos OS Release 10.4R2.

Description M120 routers with a single type-1 FPC mapped to an FEB support a microcode remap feature to resolve microcode overflow resulting in bad PIC combinations.

You can enable the microcode remap by using the **ucode-imem-remap** statement at the [**edit chassis feb slot** ***number***] hierarchy level. The default microcode map will continue to be available if the **ucode-imem-remap** statement is not configured.

NOTE: **On M120 routers, the FEB is automatically restarted once the ucode-imem-remap statement is configured and committed.**

Required Privilege Level interfaces—To view this statement in the configuration.
interfaces-control—To add this statement to the configuration.

Related Documentation

- Router Chassis Configuration Statements on page 713

vrf-mtu-check

Syntax vrf-mtu-check;

Hierarchy Level [edit chassis]

Release Information Statement introduced before Junos OS Release 7.4.

Description On M Series routers (except the M120 and 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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Enable MTU Path Check for a Routing Instance on M Series Routers on page 796
- *Junos Network Interfaces Configuration Guide*

vpn-label

Syntax vpn-label;

Hierarchy Level [edit chassis **memory-enhanced**]

Release Information Statement added in Junos OS Release 10.4.

Description Allocate more jtree memory for Layer 3 VPN labels.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Allocate More Memory for Routing Tables, Firewall Filters, and Layer 3 VPN Labels on page 792

vtmapping

Syntax vtmapping (klm | itu-t);

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure virtual tributary mapping.

Default **klm**

Options **klm**—KLM standard.

itu-t—International Telephony Union standard.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Support Channelized STM1 Interface Virtual Tributary Mapping on page 787

PART 6

Index

Index

Symbols

A

G

H

I

J

R

T

Index of Statements and Commands